

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-301904**
 (43)Date of publication of application : **13.11.1998**

(51)Int.CI. **G06F 15/00**
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : **09-345681** (71)Applicant : **SUNHAWK CORP INC**
 (22)Date of filing : **10.11.1997** (72)Inventor : **ELLER MARLIN J**
MILLS BRENT R

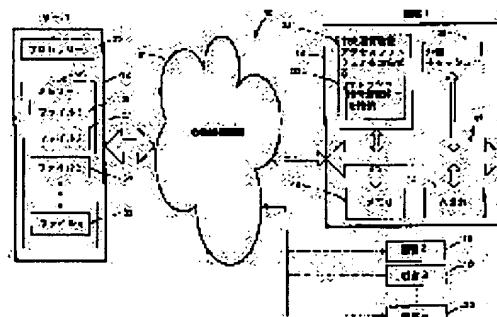
(30)Priority
 Priority number : **96 744430** Priority date : **08.11.1996** Priority country : **US**

(54) CRYPTOGRAPHIC SYSTEM PROVIDED WITH DECODING KEY MADE INTO TRANSACTION CODE

(57)Abstract:

PROBLEM TO BE SOLVED: To control access to information protected by a server and to prevent the redistribution of the information by allocating a specified key including the identifier of a customer and transmitting it to the customer so as to decode ciphered information and monitoring the distribution of the information in a customer specified base by the key.

SOLUTION: The server 12 of a computer system 10 communicates with the customers 14-20 through a public communication channel 21, receives an access request from the customers 14-20 and allocates a decoding key or a password. Then, among the information provided in the data base of the server 12, an access program protected by ciphers and the selected information (digital music score) are transmitted through the communication channel 21 to the customers 14-20. In this case, in order to decode the ciphered information in connection with the request from the customers, the specified key including the identifier of the customer is allocated and transmitted to the customer and the distribution of the ciphered information is monitored by using the decoding key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

THIS PAGE BLANK (USPTO)

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (verso)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-301904

(43) 公開日 平成10年(1998)11月13日

(51) Int.Cl. 識別記号
 G 0 6 F 15/00 3 3 0
 12/14 3 2 0
 G 0 9 C 1/00 6 6 0
 H 0 4 L 9/32

| | | | |
|---------|-------|---------|--|
| F I | | | |
| G 0 6 F | 15/00 | 3 3 0 Z | |
| | 12/14 | 3 2 0 B | |
| | | 3 2 0 E | |
| G 0 9 C | 1/00 | 6 6 0 D | |
| H 0 4 L | 9/00 | 6 7 3 Z | |

審査請求 未請求 請求項の数22 OL 外国語出願 (全 45 頁)

(21)出願番号 特願平9-345681
(22)出願日 平成9年(1997)11月10日
(31)優先権主張番号 08/744430
(32)優先日 1996年11月8日
(33)優先権主張国 米国(US)

(71)出願人 597174894
サンホーク コーポレイション インコーポレイテッド
アメリカ合衆国 ワシントン州 98112
シアトル フィフティーンス アベニュー
イースト 800
(72)発明者 マーリン ジェイ エラー
アメリカ合衆国 ワシントン州 98112
シアトル フィフティーンス アベニュー
イースト 800
(74)代理人 弁理士 中村 稔 (外7名)

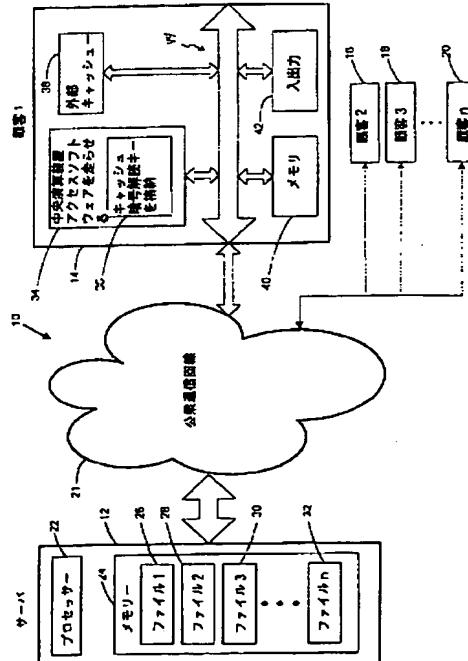
最終頁に統ぐ

(54) 【発明の名称】 取引コード化された解説キーを有する暗号システム

(57) 【要約】

【課題】 保護を掛けられた情報へのアクセスを制御し、そのような情報がサーバーから伝達された後再配布されるのを阻止し追跡するための方法とシステムを提供する。

【解決手段】 コンピューターシステムのサーバーは、保護された情報の不法な再配布を妨げ、侵害活動を追跡できる記号化された解読キーを用い、公衆通信回線を使って顧客と通信する。アクセスソフトウェア及び部分的に暗号化された楽譜が顧客の要求に応じて配布され、顧客がその楽譜を見て選定し、支払情報を入力すると、情報解読キーとして機能する特定のパスワードが割り当てられる。パスワードと共に楽譜が不法に再配布されると、パスワードの中に記号化された顧客識別情報により追跡することができる。



【特許請求の範囲】

【請求項1】 公衆通信回線を通してアクセスできる、上記公衆通信回線のサーバーにあるデータベースに含まれる情報の配布を監視するために使用する方法であって、暗号化された情報を解読するためにはキーの入力を必要とするキーをベースとした暗号化システムを使って上記情報の少なくとも最初の部分を暗号化する段階と、通信回線顧客からの要求と結びつけて、上記暗号化された情報を解読するために、上記顧客にその顧客を特定するのに使える少なくとも第1の識別子を含んだ第1の顧客特定のキーを割り当てる段階と、上記第1の顧客特定のキーをその顧客に伝達する段階とから成り、上記キーが上記情報を顧客特定ベースで配布を監視するのに使えることを特徴とする方法。

【請求項2】 上記情報がデジタル楽譜から成り、上記情報の少なくとも一部を暗号化する段階が、解読前に上記デジタル楽譜のサンプリングができるように、上記楽譜の第2の部分を暗号化されない形式に保つことから成ることを特徴とする、上記請求項1に記載の方法。

【請求項3】 上記第1の顧客特定のキーを割り当てる段階が、上記顧客に関する識別情報を取得することと、上記取得された識別情報に関する上記識別子を記号化することとから成ることを特徴とする、上記請求項1に記載の方法。

【請求項4】 上記識別子が、上記識別情報を含む顧客のデータベースに索引を付けるパスワードから成ることを特徴とする、上記請求項3に記載の方法。

【請求項5】 上記識別子が顧客の装置を特定する情報を含んでいることを特徴とする、上記請求項3に記載の方法。

【請求項6】 上記識別子が顧客ユーザーを特定する情報を含んでいることを特徴とする、上記請求項3に記載の方法。

【請求項7】 上記第1の顧客特定のキーを伝達する上記段階に先だって、上記顧客に上記暗号化された情報を伝達する段階を更に含むことを特徴とする、上記請求項1に記載の方法。

【請求項8】 顧客が上記データベース内の上記情報にアクセスできるように作動する上記アクセスソフトウェアを上記顧客に伝達する段階を更に含むことを特徴とする、上記請求項1に記載の方法。

【請求項9】 上記情報のコピーをプリントするため上記アクセスソフトウェアを使用する段階を更に含むことを特徴とする、上記請求項8に記載の方法。

【請求項10】 上記情報が楽譜のデジタル表現から成り、上記方法が上記楽譜を再生するため上記アクセスソフトウェアを使用する段階を更に含むことを特徴とする、上記請求項8に記載の方法。

【請求項11】 上記情報をディスプレイ表示する段階を更に含むことを特徴とする、上記請求項8に記載の方法。

法。

【請求項12】 上記第1の顧客特定のキーを割り当てる上記段階が上記顧客の上記要求を受け取ることに応じて行われることを特徴とする、上記請求項1に記載の方法。

【請求項13】 上記情報をメモリーの第1の領域に格納する段階と、上記第1のキーを上記第1の領域とは別の第2の領域に格納する段階とを更に含み、上記情報と上記第1のキーに別々にアクセスできることを特徴とする、上記請求項1に記載の方法。

【請求項14】 上記情報を顧客のメモリーに暗号化された形式で格納する段階と、上記情報を出力するための要求を受け取る段階と、上記出力要求に応じて上記暗号化された情報を解読する段階とを更に含むことを特徴とする、上記請求項1に記載の方法。

【請求項15】 上記情報へのアクセスを要求する第2の通信回線顧客からのアクセス要求を受け取る段階と、上記暗号化された情報の解読のために、上記第2の顧客に上記第1の顧客特定のキーとは異なる第2の顧客特定のキーを割り当てる段階とを更に含むことを特徴とする、上記請求項1に記載の方法。

【請求項16】 上記情報の統いて起こる再配布を追跡するため上記第1の顧客特定のキーを使用する段階を更に含むことを特徴とする、上記請求項1に記載の方法。

【請求項17】 上記情報の出力コピーを出力する段階と、識別情報を上記出力コピーに埋め込む段階とを更に含み、上記識別情報が上記情報の再配布の追跡をやり易くすることを特徴とする、上記請求項1に記載の方法。

【請求項18】 公衆通信回線を通してアクセスできる保護された情報の配布を監視するのに使用するコンピューターシステムであって、上記保護された情報を含むデータベースを格納するためのメモリーの第1領域と、上記保護された情報へのアクセスを要求する通信回線顧客からのアクセス要求を受け取り、ソースを特定するのに役に立つ識別情報を得て、上記識別情報を使って暗号解読キーを割り当てるよう作動するコントローラーと、上記暗号解読キーに基づいて上記保護された情報を暗号化するための暗号化ロジックとから成り、上記暗号解読キーが上記暗号化された保護された情報を解読するのに役立つことを特徴とするコンピューターシステム。

【請求項19】 上記識別情報を格納するためのメモリーの第2領域を更に含み、上記識別情報が上記暗号解読キーに索引を付けることを特徴とする、上記請求項18に記載のコンピューターシステム。

【請求項20】 上記コントローラーが顧客からの支払情報を受け取るよう作動し、上記暗号解読キーが上記支払情報の受け取りに応じて割り当てられることを特徴とする、上記請求項18又は19の何れかに記載のシステム。

【請求項21】 上記保護された情報をディジタル楽譜

から成り、上記暗号化ロジックが上記楽譜を部分的に暗号化するように作動することを特徴とする、上記請求項18、19、20の何れかに記載のシステム。

【請求項22】 ソースが上記通信回線顧客であることを特徴とする、上記請求項18、19、20、21の何れかに記載のシステム。

【発明の詳細な説明】

【0001】

【産業上の技術分野】 本発明は大体において、公衆通信回線を通してアクセスできる配布情報を監視すること、特に、キー所有者による公認されていない配布を禁止、追跡するためのキーをベースとした暗号を使用する方法とシステムに関する。本発明は著作権のある作品又はその他の所有権のある内容物の公衆通信回線を通しての商業的配布に関して特に適用されるものである。

【0002】

【発明の背景】 広範囲に利用できるコンピューター公衆通信回線、特にインターネットのようなマルチメディア機能を支援することのできる公衆通信回線の出現は、消費者及び音楽出版社のようなコンテンツプロバイダー

(情報中身の作成者)に大きな機会を提供している。このようなネットワークのおかげで、コンテンツプロバイダーは成長し続けるマーケットに今まで以上にアクセス出来るようになった。消費者は情報にアクセスし易くなり、大変便利になった。更に、ある場合には、ネットワークを通して得られる情報のデジタル特性の方が、印刷されたメディアのような従来型の情報よりも好ましいことがある。例えば、デジタルシート音楽はその印刷されたメディアの複写を複製するために印刷することもできる。加えて、デジタルシート音楽は、ミディ(MIDI:電子楽器間のデジタルインターフェース)装置のような様々なデジタルの楽器と装置によってと同様に、オーディオやビデオの再生プログラムによっても直接処理することができる。

【0003】 このような可能性があるにもかかわらず、コンテンツプロバイダーは多くの場合このマーケットを利用するのを躊躇している。この躊躇の理由の一つは、公衆通信回線を通しての著作権のある音楽のような所有権のあるものへのアクセスはそのような内容物からの所有者の利益と収入を侵すことになるだろうという恐れがあつたからである。この懸念はつまり、不謹慎な人々がそのような内容物に不法にアクセスしたり、或いは承認されたユーザーが内容物に正規にアクセスした後その内容物をコンテンツプロバイダーの権利に違反して配布するという懸念である。そのような可能性は他の配布の形式と結びついて存在するけれども、公衆通信回線配布は、掲示板等のように広範囲な配布のできるその容易さの故に特異な危険性をもたらすものであると考える人もいる。

【0004】 事実、アクセスの制限されているデータへ

のアクセスを制御するために開発された従来のコンピューター機密保全システムは、コンテンツプロバイダーのこうした懸念に適切に対応していない。例えば、アクセスパスワードシステムは指定された情報へのアクセスを制限するのにはある程度効果的であるが、情報が一旦サーバーシステムから公衆通信回線に伝達されてしまうと保護を掛けすることはできない。暗号システムは通信回線を通しての伝達の結果として不法に盗聴される情報の使用を阻止するために考案されたものである。この事に関しては、キーをベースとした暗号システムでは、承認された顧客には解読キーが提供される。それから、盗聴者の使用を妨げるために、保護を掛けられた情報が暗号化された型式で伝達されることになる。承認された顧客は暗号化された情報を受け取り、解読キーを使って情報を解読する。不幸にも、通常このような暗号システムは、承認された顧客が保護を掛けられた情報を受け取った後で再配布するのを妨げる適切な防御策を提供してはいない。

【0005】

【0006】 【発明の概要】 本発明はサーバーからの保護を掛けられた情報へのアクセスを制御し、又そのような情報がサーバーから伝達された後再配布されるのを阻止し追跡するための方法とシステムを目指したものである。本発明は、所有権の保護を改善し、侵害する活動を是正する機会をふやすことにより、所有権のある内容物の公衆若しくは解放通信回線を通しての商業的配布をやり易くするものである。更に、本発明は、限定された多重使用の承認と、著作権のある作品又は他の機密内容の購入前サンプリングを考慮することによって、市場取引の柔軟性を増やすようしている。本発明は又、CD-ROM及び磁気記憶媒体のような物理的な記憶媒体と結びつけての実現性はないと考えられてきた、今までにない暗号即応能力を提供する。

【0006】 本発明のある態様では、顧客特定ベースの公衆通信回線を使ってアクセスできる情報の配布を監視するための方法及び対応するシステムを提供する。この方法には、サーバーで情報のデータベースを確立する段階と、キーベースの暗号システムを用いて情報の少なくとも一部を暗号化する段階と、顧客の要求と関係付けて顧客に顧客特定のキーを割り当てる段階と、キーを顧客に伝達する段階とが含まれている。顧客特定キーには、顧客を特定するのに使え、それによって顧客特定ベースでの情報の使用を監視することのできるある種の印が含まれている。データベースには、例えばデジタルシート音楽、文学又は芸術作品、ソフトウェアプログラム、その他のデジタル形式で伝達できる内容物等、様々な情報を入れることができる。どのような識別情報でも顧客識別のキーにコード化して入れておくことができる。例えば、顧客の提供した個人的又は財務的な情報、顧客のコンピューター又はウェブサイトのためのアドレス情

報、アカウントナンバー又はセリアルナンバー、顧客の使用するコンピューターを識別するためのその他の情報、以上の情報を省略表示又は暗号化したもの、等々である。便利なことに、このような情報は別々の顧客のデータベースの中に記憶させキーに索引を付けておくことができる。暗号解読システムは、保護された情報が使用される度に入場許可のキーを必要とし（即ち、システムは情報を解読された型式では記憶しない）、再配布されるデジタル情報或いは情報のハードコピー全てに顧客識別情報が添付されるのが望ましい。こういう方法にすれば、情報をその元のデジタル型式で使用するためにキーが必要であり、キー又は識別情報の付いたハードコピーを配布することは機密情報を開示することになるか、さもなければ顧客の侵害行動を追跡できる記録を作り出すことになるので、保護された情報を顧客が再配布することを阻止できる。

【0007】又、本発明の他の態様では、保護された情報に関して取引特定のアクセス承認ができるようにする方法及び対応システムが提供されている。この方法には、暗号解読キーが取引毎ベースで割り当てられる、先に概ね述べたような、キーをベースとした暗号システムを使うことが含まれている。即ち、保護された情報をサーバーから顧客へと通信することを含む取引と関係する要求に即して、キーが割り当てられる。例えば取引には、シート音楽のコピー、デジタル音楽の楽譜、或いは他の保護された情報の購入が含まれていてもよいし、そのような情報を指定した回数、指定した期間、或いは指定したライセンスの期間使用するためのライセンス料金が含まれていてもよい。キーには対象情報及び/又は顧客を識別するのに十分な情報を含ませておくことができる。本発明はこれによって、取引特定の承認ができるようになり、市場取引/配布の可能性を拡大する。

【0008】本発明の又他の態様では、解読キーを提供するに先だって部分的に暗号化された情報を伝達し、取引が成立する前に情報のサンプリングができるようにしている。特に、一緒に付いている方法には、通信回線サーバーで情報のデータベースを確立し、情報の一部を暗号化し、アクセス要求を受け付けることが含まれている。アクセス要求の受付に応じて、情報の選択された部分が部分的に暗号化された型式で伝達され、その後、解読キーが顧客に伝達される。例えば、部分的に暗号化された情報とは、楽譜の最初の頁だけが見られるように暗号化されていないシート音楽であってもよい。これによって顧客は購入を決めるに先立って楽譜の選択にざつと目を通して、支払を承認し、それと引き替えに解読キーを受け取ることができるようになる。

【0009】本発明の更に他の態様では、情報を伝達後に顧客がどう使うかを監視することができる方法と対応するシステムを提供している。この方法には、暗号化された情報を受信しその情報を暗号化された型式でメモリ

一に格納する段階と、解読キーを受信しそのキーを暗号化された情報とは別のメモリー例えばキャッシュに格納する段階と、情報にアクセスするための顧客の要求を識別する段階と、要求に応じてメモリーから暗号化された情報とキーとを検索して、それから情報を解読する段階と、情報を顧客の使用に供するために出力する段階とが含まれている。この方法は、例えば顧客のコンピューター上で走る再生/ディスプレイ表示のソフトウェアで実行させることができる。このソフトウェアは、取引のパラメータに応じて保護された情報へのアクセスを制限する、即ち顧客が購入したライセンスの範囲にアクセスを制限するようにプログラムすることができる。

【0010】好ましい実行形態では、保護された情報は決して解読された型式でセーブされることではなく、対応するファイルが使用に供するために開かれるときにジャストインタイムで解読されるだけになっている。従つて、情報を解読された型式で再配布することは思い止まられ、或いは実際には阻止される。更に、第三者が情報を使用出来るようにするために、暗号化された型式での情報の配布も解読キーの配布を必要とし、これは顧客にとって興味を引く選択ではなかろう。このように本発明は、サーバー上の保護された情報へのアクセス、それに続く顧客の使用或いは再配布を監視できるようにする。更に、本発明は承認されていない再配布を全て追跡できるようにするので、サーバーの権利を強化するのに役立つ。本発明は又、市場取引/配布の機会を増やし、今までにない要求即応型の解読キーのコード化ができるようになる。これらのそしてその他の利点によって、本発明は所有権のある内容物を公衆通信回線を通して配布し消費者及びコンテンツプロバイダー双方の利益に供することを促進する。

【0011】本発明の配布/監視システムは、所有権のある内容物の公衆通信回線を通じての配布を監視することが必要な様々な場面で役に立つ。以下の説明において、本発明を、通信回線を通してのデジタルの楽譜の配布を監視するという状況下で説明する。この特定の適用例は説明の目的で取り上げるのであり、本発明の様々な態様が請求の範囲で規定する広範な適用範囲を有していることは理解頂けるであろう。図1は本発明により暗号で保護されたコンピューターシステム10を示す。コンピューターシステム10にはインターネットのような公衆通信回線21を通して顧客14-20と通信できるサーバー12が含まれている。インターネットの場合、サーバー12にはネットスケープ2.01又はマイクロソフトのインターネットエクスプローラー3.0或いは更に上位のブラウザを使ってアクセスできる。一般にサーバー12には、プロセッサー22と、ファイル26-32としてメモリー24に記憶されているデジタル楽譜のライブラリー或いはデータベースとが含まれている。以下で詳細に論議するが、サーバー12は顧客14

—20からのアクセス要求を受け付け、解読キー又はパスワードを割り当て、通信回線21を通して顧客14—20へアクセスプログラムと選択された楽譜とを伝達するように作動する。支払を受け付け、暗号化された解読パスワードを検索し、記憶する等のことに関する他の数々の機能もサーバー12が行う。

【0012】現下の目的に対して、顧客14—20は機能的には等価であると考えてよい。顧客の一人14についてだけ詳細を図1に示す。一般的に顧客14には、中央演算装置(CPU)34、内部キャッシュ36及び／又は外部キャッシュ38、メモリー40、入出力(I/O)ハードウェア42が含まれ、全てがデータバス44を経由して相互に接続されている。CPUは適当なマイクロプロセッサーを含んでいてもよく、アクセスプログラムをダウンロードして走らせ、メモリー40とキャッシュ36及び38にアクセスし、入出力ハードウェア42と通信するように機能する。図解した実施例では、CPU34にはダウンロードされた楽譜を解読するために使う解読キーを記憶するための備え付けの内部キャッシュも含まれている。一般的に、キャッシュ36は、より早い作動ができるように、しばしば使用される或いは時間的にクリティカルなデータを記憶するための、極最速のランダムアクセスメモリー(RAM)領域にある。キャッシュ36にはメモリー40よりもより迅速にアクセスできる。替わりに、解読キーは外部キャッシュ38に格納させることもでき、これはコンピューターのマザーボード上に配置されたRAMチップから成っていてもよい。メモリー40はキャッシュ36及び38とは別で、フロッピーディスク、CD-ROMドライブ、ハードドライブの記憶装置の他コンピューターのメモリーを含んでいてもよい。入出力ハードウェア42には、マウス、キーボード、他のユーザー入力装置、視認用モニター、プリンター、ミディ装置等を始めとした様々な型式の装置が含まれる。

【0013】図2は図1のコンピューターシステム10と組み合わせて使用される音楽配布監視システム46の機能的概要を示す。図2に示すように、監視システム46は、サーバー及び／又は顧客のコンピューターのロジックで実行される多くの機能に細分化することができる。図解したシステム10の機能には、サーバーに記憶されている音楽ファイルに顧客がアクセスするのに使う、この場合には「ミュージックビューアー」と明示されている、音楽アクセスプログラムをダウンロードすること(48)、サーバーから選定した楽譜をダウンロードすること(50)、オンラインで音楽を購入すること(52)（そしてこれによってアクセスライセンスと暗号化された解読キーを得ること）、音楽及び音楽の暗号化／解読をプリント(54)及び／又は観察すること(56)が含まれる。音楽は、ミディ装置などを使ってデジタル情報から再生できることが理解できるであろ

う。これらの機能各々を以下に論議する。

【0014】図3に本発明の一つの実行例であるミュージックビューアーのダウンロード機能を示す。サーバーと顧客との間の通信が通信回線を経由して確立した後、顧客はサーバーにプログラムをダウンロードすることを要求して(58)ダウンロード機能を始動する。この要求はサーバーサイトからの適切な指示メッセージに従つて入力することができる。サーバーはダウンロード要求を受け取り(60)、顧客にビューアーのソフトウェアパッケージを送る(62)。顧客はソフトウェアパッケージを受け取る(64)と、ミュージックビューアーのソフトウェアをインストールするためのセットアップコードを走らせる。図示されているシステムのサーバーライブラリーの中に記憶されている楽譜にアクセスするため、顧客には固有のビューアー識別コードが割り当てられる。従つて、顧客はダウンロード手続きの一部としてビューアーIDを要求する(66)ように促される。ID要求に応じて、サーバーはビューアーIDを作つて(68)そのIDをビューアーのデータベースに記録する。次にサーバーは新しく作ったビューアーIDを顧客に送り(70)、伝達日時、顧客のインターネットプロトコル(IP)アドレス（又は、他の通信回線用の同等の情報）、顧客の装置の名称又は型式（顧客の入力によって、又は伝達ヘッダー等から決めて）を記録する。次に顧客ユーザーは割り当てられたビューアーIDを受け取り(72)、これで導入が完全に済んだことになる。

【0015】図示した実施例のシステムでは、顧客ユーザーは音楽のコピーを購入し或いはライセンス料金を支払って取引を成立させるに先立つて、音楽ライブラリーの中を概観し、楽譜の選定された部分即ち最初の頁を見ることができる。図4は一緒に付いている購入前音楽ダウンロード機能を示している。この機能は顧客が試聴する楽譜を選定しサーバーからの音楽を要求した(74)ときに始動する。この場合、楽譜は、ライブラリーをスクロールして選定したタイトルの上でクリックして、又はタイトルを呼び出すための検索機能を使って、或いはその他の適切な手段で、タイトルのリストから選定すればよい。ビューアーIDもこのときにサーバーへ送られる。要求を受け取ると、サーバーは要求された楽譜を探し出して(76)、以下に説明するように楽譜を圧縮及び暗号化し（又は部分的に暗号化し）、暗号化した楽譜をダウンロード領域に格納する。更に、サーバーは顧客に固有の解読キーを割り当てそして記録し、楽譜、ダウンロードIP、伝達用のビューアーIDのための識別コードも記録する。例えば、キーは、1つの番号が顧客データベースで顧客を特定するためのインデックスであり、もう一つの番号がランダムな或いは必要な追加情報で記号化されたものである、2つの32ビットの数で構成されたパスワードであつてもよい。この方法で顧客データベースにキー或いはパスワードの索引を付ければ、

パスワードは顧客を特定し、ライセンス又はアカウント情報を調べるのに使うことができ、その他、顧客特定及び取引特定ベースで配布を監視することもできる。

【0016】それからサーバーは新しく暗号化された音楽のユニフォームリソースロケーター(UR L)のアドレスを顧客に送る(78)。顧客はUR Lを受け取ると(80)、暗号化された音楽を含むファイルのダウンロードを要求する(82)ことができる。するとサーバーはダウンロード領域の中で暗号化された音楽を見つけ出し(84)、音楽を待ち行列に入れ、そして音楽を顧客にダウンロードする(86)。顧客は暗号化された音楽を受け取り(88)、音楽をコンピューターメモリー、ハードドライブ記憶装置などのメモリーに記憶させる。図解実行例ではこの時点、即ち購入前では、楽譜の最初の頁だけが暗号化されていない。従って、顧客ユーザーは音楽の最初の頁を演奏しそして見てみて(90)ダウンロードされた楽譜がユーザーの望んだ楽譜であることを確かめ、或いは、購入のオプションを評価することができる。

【0017】この様に音楽ライブラリーをざっと見渡し、1つ或いはそれ以上の楽譜を抜き出してみた後で、顧客ユーザーはオンラインでの音楽購入、例えば音楽のコピーをシート音楽の型式で購入するか、ライセンス料を払ってコピーをプリントし、音楽をそっくりそのままの状態で見て、顧客の入出力ハードウェア上で音楽を再生するか、或いは音楽を他に使うかを決めればよい。ライセンスには、一回だけの使用、多数回の使用、ライセンス期間内での無制限の使用等があつてもよい。図5にオンライン購入機能を示す。この機能は顧客が支払情報(例えば、クレジットカードのアカウント番号と有効期限、或いはサーバーの設立した予め確立されている前払い又は非前払いアカウント)、楽譜のID、ダウンロードID、ビューアーID及び/又は何か他の情報をサーバーに送る(92)ことによって始動する。この情報の幾つか又は全部は音楽ライブラリーを概観する際にサーバーに伝達するようにしておいて、再伝達する必要がないようにしておくこともできる。個人的及び財務的情報の交換は、例えば、ブラウザのセキュアソケットリヤー(SSL)の中で提供されている標準的な公共キー暗号を使って暗号化することができる。

【0018】サーバーはこの情報を受け取る(94)と、楽譜とビューアーIDをダウンロードし顧客ユーザーの財務機関或いはクレジットカード承認サービス機関と接触し、収支情報を調べ、又は他のやり方で取引承認を得る。この承認調査の結果に基づいて、サーバーは顧客に不良支払メッセージ(例えば「支払が拒絶されている」)或いは解読パスワードを送り(96)、パスワード及びその他の取引情報をデータベースに記録する。ミュージックビューアーのソフトウェアを働かせることによって、顧客は次にパスワードを受け取って(98)、

それをダウンロードされた音楽とは別のパスワードデータベースに格納する。このように、一般的にユーザーは解読パスワードがそのシステム内に格納されていることを分かっておらず、又ユーザーはどのようにしてパスワードにアクセスするのかを知らないので、顧客ユーザーが不適切に音楽を再配布するのは困難である。作動すると、ミュージックビューアーのソフトウェアは、ユーザーが音楽をプリント、再生或いは他に使うことを望むことを表示する「オープンファイル」メッセージ受け取る

10 (100)まで顧客のメッセージをモニターする。このときミュージックビューアーはパスワードの配置を決める(102)が、それは作動の速度を上げるため顧客のキャッシュに格納しておくこともできる。ミュージックビューアーは顧客のアクセス要求に関係するライセンス情報を検索することもできるし、適切な場合には、以下に述べるようにライセンス下での顧客の使用回数を積算することもできる。顧客がライセンス下での使用回数を残している場合は、ミュージックビューアーはメモリーの楽譜を暗号解読する。音楽は決して暗号解読された型

20 式でセーブされているのではなく、使用要求に応じてジャストインタイムで解読されるのであり、これによって不正な再配布を阻止するということに留意しておくべきである。

【0019】図6は本発明による音楽プリント機能を示している。先に述べたように、音楽とパスワードをダウンロードした後、ミュージックビューアーはアクセス要求を特定するため顧客のメッセージをモニターする。プリントコマンドを受け取った(104)場合、ミュージックビューアーは、顧客データベースから情報を取つ

30 て、顧客ユーザーが予め購入したライセンスの下で許されるプリントアウト回数がまだ残っているか否かを決める(106)。この場合、顧客ユーザーは單一回使用又は複数回使用のライセンス料金を既に支払っているはずである。ライセンスを既に使い切っている場合は、顧客にはその旨通知され(108)、更にライセンス料を支払う選択をするか否かについての情報が提示される。でなければ、ミュージックビューアーは、ビューアーID、楽譜ID、ダウンロードID、日付、時間、ライセンスされ使用されたプリントアウト回数等のユーザーデータベース内の取引に関する種々の情報を記号化する

40 (110)。この情報は、例えば72を底とする記号列に適切な書式で記号化し、それからコピー(例えば、版権表示の次)にプリントする(112)ことができる。同様に、この同じ識別情報を、MIDI引き出しにタグを付けるためにMIDIファイルの注釈ステートメントに書き込むこともできる。この情報によって、多数回使用ライセンスの正しい積算を行うことができ、引き続いて、プリントされたコピーの不法な再配布を全て追跡することができる。この場合、楽譜又はMIDIファイルのコピーが見つかれば、これに関わる取引及び顧客

を容易に解読することができる。

【0020】音楽をプリントする替わりに、或いはそれに加えて、オンラインユーザーは音楽をモニター上で見たいと思うかもしれない。例えば、楽しみを増すために音楽を再生すると同時に音楽を見る事もできるし、テンポ、器楽編成等を始めとする再生選択事項の選定をやり易くするため、音楽をディスプレイ表示することもできる。図7は一緒になっている音楽観察機能を示す。ディスプレイ表示コマンドを受け取る(114)と、ミュージックビューアーは要求された音楽ファイルを開き(116)、ファイルが暗号化されているか否かを確認する(118)。例えばその音楽が前のステップで解読済みであったり、或いは権利消滅音楽であったりして暗号化されていない場合、音楽は直接ディスプレイ表示(124)することができる。しかし、サンプリングのための最初の1頁を除いて音楽が暗号化されている場合、ミュージックビューアーは最初の頁をディスプレイ表示し(120)、プリント又はMIDI引き出しができないようにする。顧客ユーザーがそれから音楽の残り部分をディスプレイ表示しようとする場合、ミュージックビューアーは先ず、有効且つ満了していないパスワードがユーザーに割り当てられているか否かを確認する(122)。割り当てられていれば音楽は解読されてディスプレイ表示される(124)。そうでない場合、エラーメッセージがディスプレイ表示される(126)。

【0021】図8、9に音楽配布監視システムの暗号化／暗号解読機能の一つの実行例を示す。公共キー暗号化／暗号解読アルゴリズムの使用を含め、適当な技法であればどんなものでも、本発明に従ってベースレベルの暗号化／暗号解読技術として使用できることは理解頂けるであろう。更に、ベースレベルの暗号化／暗号解読技術はハードウェア及び／又はソフトウェアのロジックで実行できる。以下の説明では一つの代表的実行例を示す。先ず図8には、暗号化／暗号解読の構成要素が概略表示してある。サーバー側では、暗号化／暗号解読サブシステム126に圧縮ロジック128、ランダム番号発生器130、排他的OR(XOR)ゲート132が含まれている。圧縮ロジックは従来型のデータ圧縮ソフトウェアプログラム又はデータ圧縮ハードウェアパッケージであってもよく、生のデジタル楽譜を受け取り伝達のため楽譜を圧縮する。この圧縮によって伝達速度が改善されるばかりでなく、圧縮され暗号化されたデータは盗聴者が解読するのが特に難しいので、それに続く暗号化の意味が増す。ランダム番号発生器130には1つ又はそれ以上のランダム番号発生プログラムが含まれていてよい。この場合、暗号解読パスワードの2つの32ビットのワードを処理するために2つのそのようなプログラムを使用することができる。ランダム番号発生器130は最初の種から出発して決められた数値の列を作るためのアルゴリズムを実行する。図解した実施例では、割り当

てられたパスワードが種として発生器130に渡される。発生器130は又、圧縮されたデータの流れと長さが等しくそれと統合されたビットの流れを発生器130が outputするように発生器130の引き金を引く圧縮されたデータの流れの行から入力を受け取る。発生器の出力及び圧縮されたデータの流れは、特性論理和コンパレータ機能を実行するXORゲート132への2つの入力として使用される。XORゲート132からの出力は通信回線を経て顧客に伝達される。

10 【0022】顧客側ではサブシステム126に顧客側のランダム番号発生器134と顧客側のXORゲート136が含まれ、各々がそのサーバー側の相手と一致している。サブシステム126には更に、圧縮ロジック128の論理補数となる圧縮解凍ロジック138が含まれている。ランダム番号発生器134はパスワードを種として使い、暗号化されたデータの流れからの入力によって長さが決められたビットの流れを作る。発生器134からの出力ビットの流れは発生器132からのものと同じで、この出力と暗号化されたデータの流れはXORゲート136への2つの入力となることは理解頂けるであろう。XORゲート132及び136の連続した作動によってXORゲート136からアウトプットが出てくるが、これは圧縮ロジック128からのアウトプットと同じで、即ち、圧縮された楽譜である。この圧縮された楽譜は圧縮解凍ロジック138で解凍され、圧縮されていない、解読された型式でデジタル楽譜が生み出される。楽譜は音楽出力処理の一部として暗号解読されているのであり、楽譜をセーブする前に解読されるのではないことに留意しなければならない。更に、暗号化／暗号解読の処理は、準備されたベースでのディスプレイ表示／再生ができるように、プリントの場合にはページサイズの塊で、或いはオーディオ出力の適当なサイズの部分毎に(例えは楽譜2秒分)継続して行われる。

【0023】暗号化／暗号解読の処理は図9のフローチャートにまとめてある。処理は、サーバー側で、楽譜のデジタル表現を受け取る(140)か、メモリーから呼び出すかすることで始まる。それから、デジタル表現は、順に、圧縮され(142)、暗号化され(144)、通信回線を経て顧客に伝達される(146)。顧客側では、信号は先ず、圧縮されたデジタル表現を得るために解読され(148)、それからデジタル楽譜を得るために圧縮解凍される(150)。そうすると楽譜は顧客ユーザーが望んだように出力される(152)。以下の予言的例は本発明の音楽配布監視システムの全作動を示すものである。顧客は音楽配布サーバーに、例えはマイクロソフトのインターネットエクスプローラー3.0ブラウザを使って、そのワールドワイドウェブ(WWW)サイトでアクセスする。ユーザーは最初、サーバーのホームページからミュージックビューアープログラムをダウンロードするためのオプションを選

20

30

40

50

択する。このオプションを選ぶと、ユーザーは指示又は命令に従ってソフトウェアをインストールし、処理の過程で、要求される各種の識別データを入力する。ユーザーはそれからホームページに帰り、音楽ライブラリーオプションを選択して利用できる選択項目にざっと目を通してよい。それから、ユーザーは利用できる選択項目をスクロールして、例えば、「モーツアルトのソナタ第1」というふうに、興味のある楽譜を特定することができる。ユーザーはそれが自分の考えているものであるということを確かめるために、サンプリングのため楽譜をダウンロードしてもよい。ミュージックビューアーのソフトウェアは部分的に暗号化されたデジタル楽譜を記憶して、楽譜の最初のページ（これは暗号化されていない型式で伝達される）を顧客のモニター上にディスプレイ表示し、再牛できるようしている。

【0024】このようにして1つ或いはそれ以上の楽譜をサンプリングした後、ユーザーはデジタル楽譜をプリントするか、見るか、他に使うかを決め、楽譜のコピーを購入するか、ライセンス料を支払うかを決めることができる。それからユーザーは購入機能を選択することができ、例えば、單一回プリントのライセンス、複数回プリントのライセンス、所定のライセンス期間の間無制限に見るライセンス等の購入オプションのメニューが提示されることになる。ユーザーは所望のオプションを選択し、クレジットカード番号及び個人情報を入力する等して、識別情報及び支払情報に関する一連の質問に応える。支払が承認されると、サーバーが保持する顧客データベースの中の顧客識別情報への索引が付いた暗号解読パスワードがユーザーに割り当てられる。例えば、顧客は10回のプリントアウトに対してライセンス料を支払ってよい。同一の又は次のセッションで、顧客はライセンス下でのプリントアウトを要求することができる。このシステムは使用されたプリントアウトの回数を追跡し、ライセンスが使い尽くされていない限りプリントできるようにする。ユーザーが楽譜のコピーをプリントアウトするときには何時でも、記号化された文字列が版権表示の次にプリントされる。

【0025】不心得なユーザーは、サーバー／版権所有者の権利に無頓着に音楽を再配布しようとするかもしれない。自分のシステムにダウンロードされた音楽のファイルを持っているので、ユーザーは、音楽を電子的に再配布しようとするかもしれない。しかし、このように不

法に音楽を再配布しようとなれば、ユーザーは、再配布された情報が暗号化されているため使用できないことが分かることになる。そのようなユーザーは暗号化コードを破ろうとして、最後には、音楽ファイルとは別の顧客のメモリーのどこかにキーが格納されていると推測するかもしれない。ユーザーが使える形のパスワードと共に音楽を再配布するのに成功するという起こりそうにないことが起きた場合、侵害したユーザーは、顧客／取引暗号化パスワードから導き出せる個人情報の形式の中に自分の侵害行動の記録を気付かず残していることになるだろう。同様に、プリンとされたコピー又はMIDIファイルを再配布すれば、版権表示と共に或いは注釈ステートメントの中に含まれる記号化文字列のために記録を提供することになる。何れの場合も、記号化された情報は実施をやり易く、こうして侵害を妨げる。

【0026】以上、本発明の様々な実施例と応用例を詳細に説明してきたが、本発明には更なる変更及び適用ができるることは当業者にとって明らかである。しかし、そのような修正と適用が本発明の精神と範囲の中にあることは、明確に理解されなければならない。

【図面の簡単な説明】

本発明及びその更なる利点のより完全な理解のために、次の詳細な説明の項で以下の図面を参考にしながら解説を行う。

【図1】図1は本発明によるコンピューターシステムの図解線図である。

【図2】図2は本発明の配布監視システムの機能概観を示すチャートである。

【図3】図3は図2のシステムのミュージックビューアーのダウンロード機能の線図である。

【図4】図4は図2のシステムのミュージックダウンロード機能の線図である。

【図5】図5は図2のシステムのオンライン音楽購入機能の線図である。

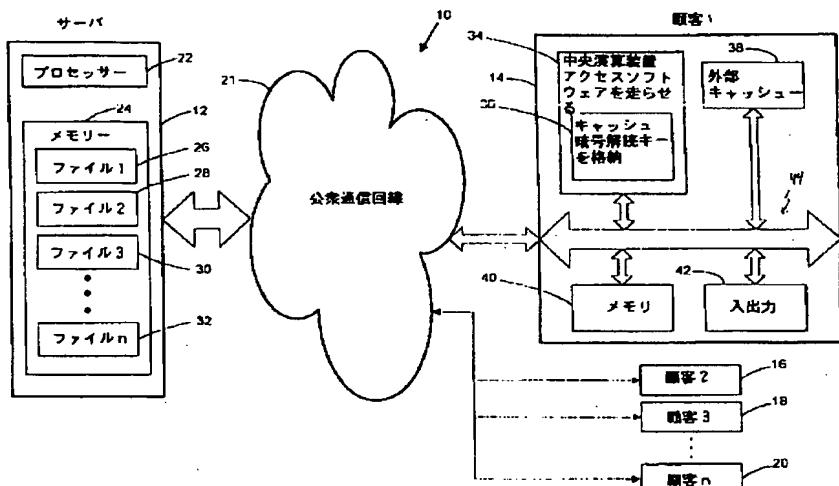
【図6】図6は図2のシステムの音楽プリント機能のフローチャートである。

【図7】図7は図2のシステムの音楽観察機能のフローチャートである。

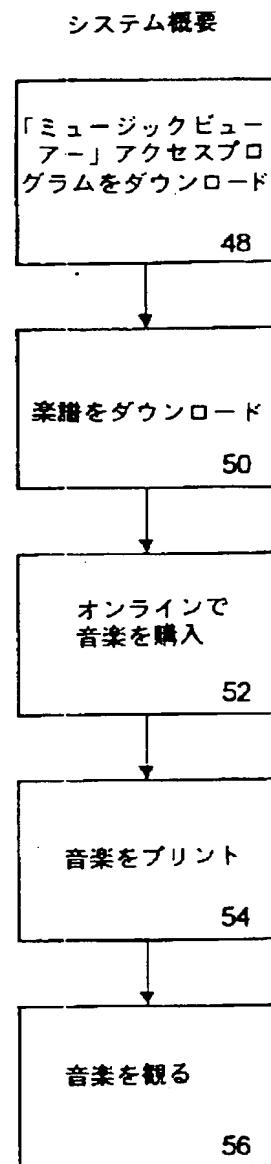
【図8】図8は図2のシステムの暗号化／暗号解読の構成要素の図解線図である。

【図9】図9は図2のシステムの暗号化／暗号解読機能のフローチャートである。

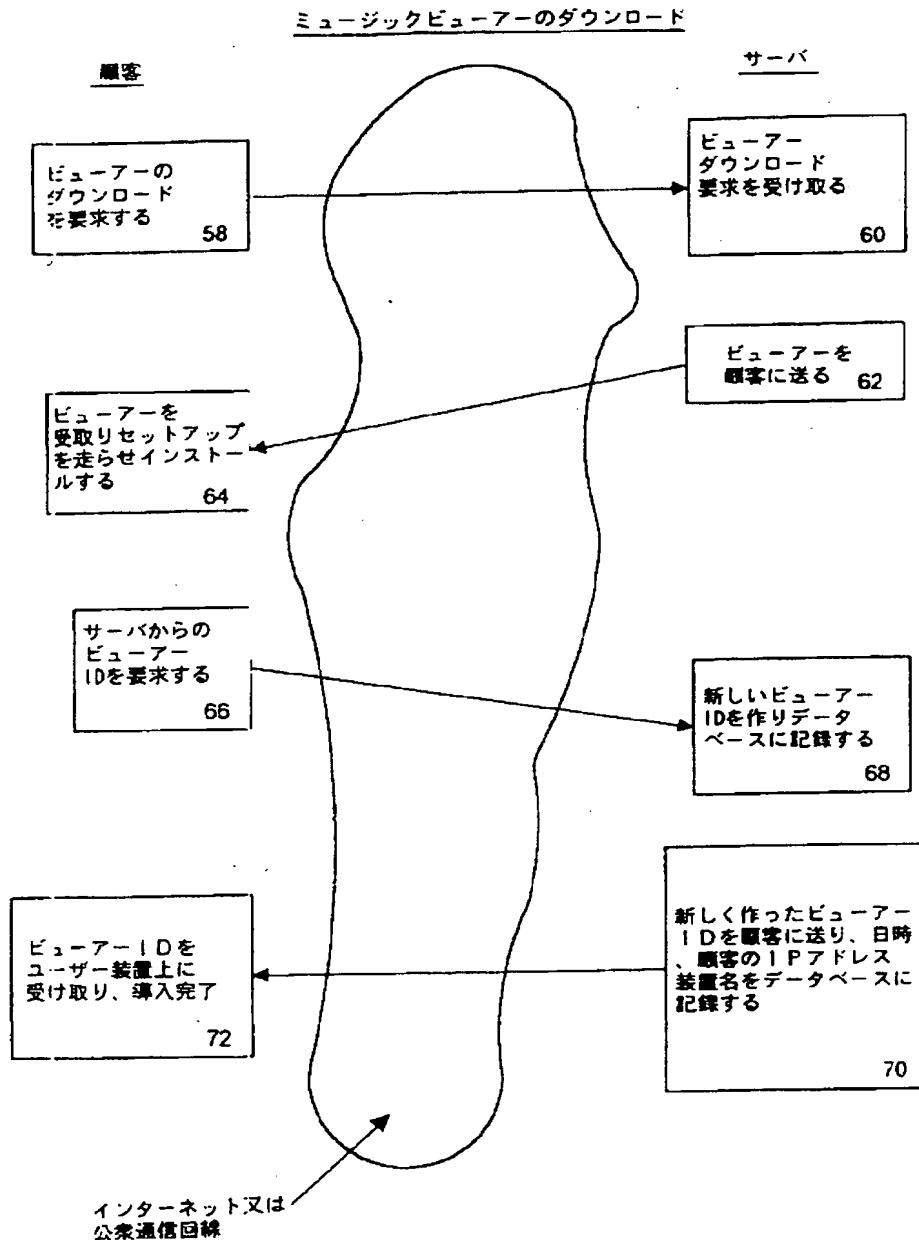
【図1】



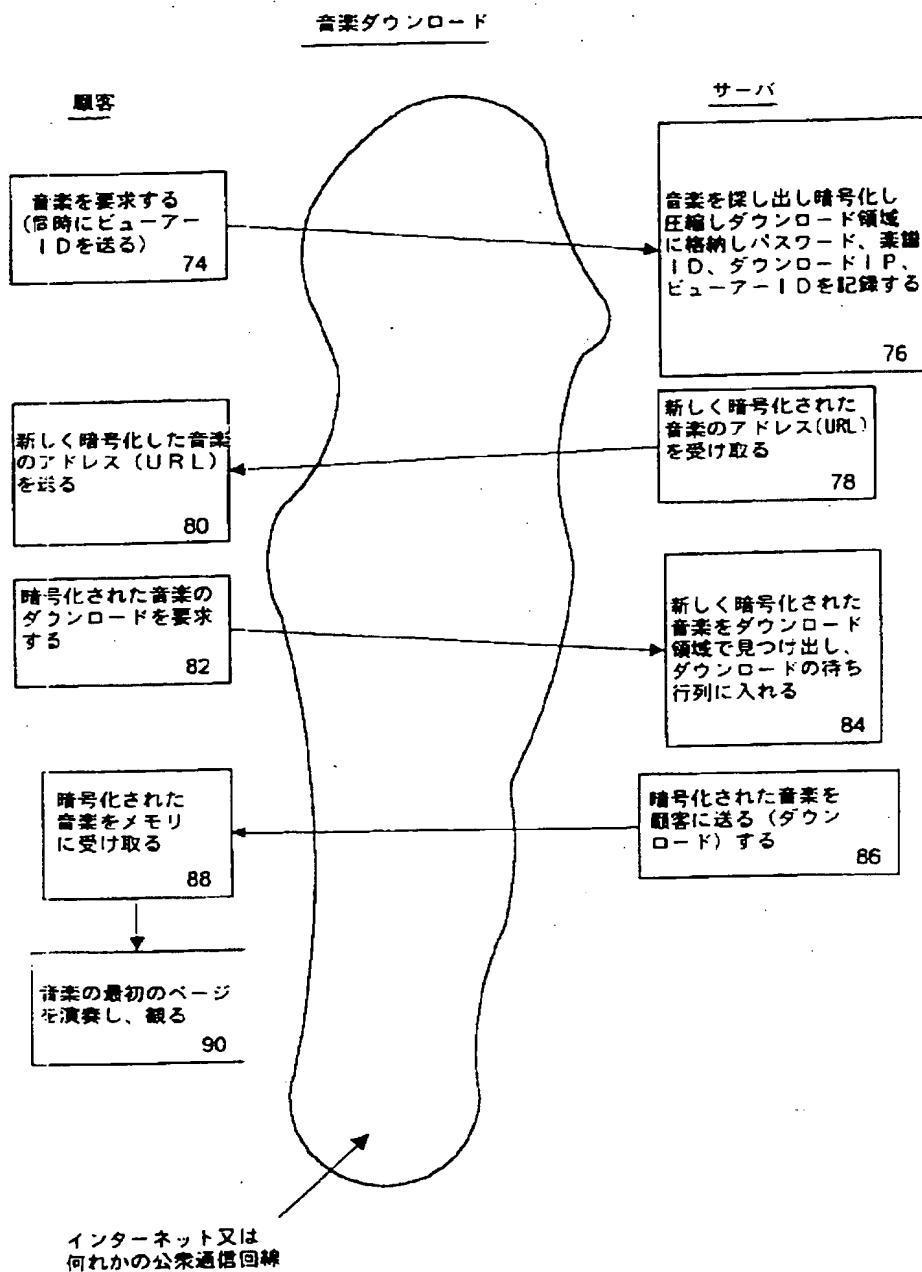
【図2】



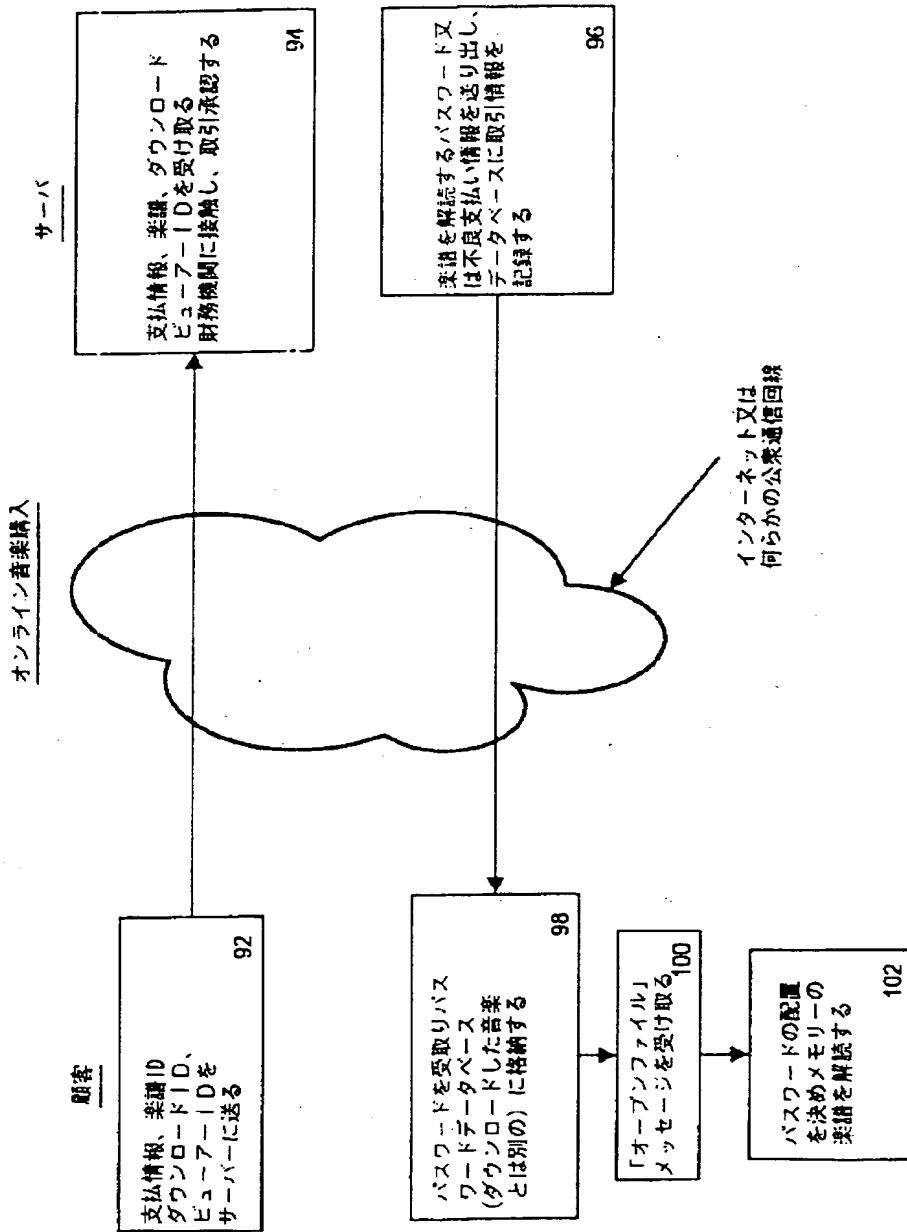
【図3】



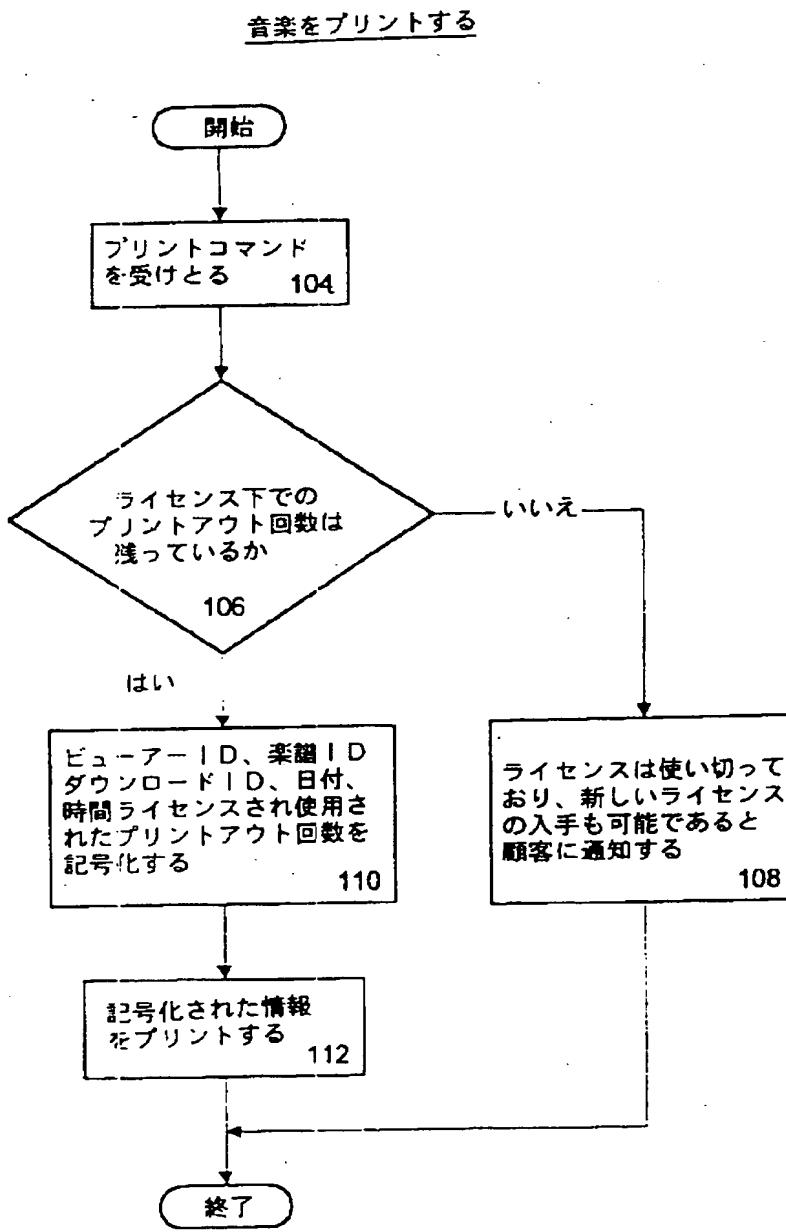
【図4】



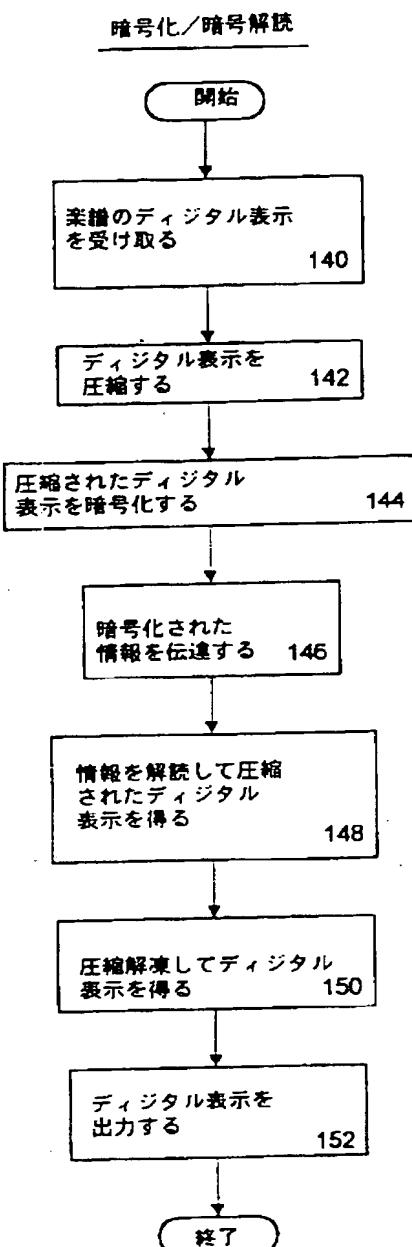
【図5】



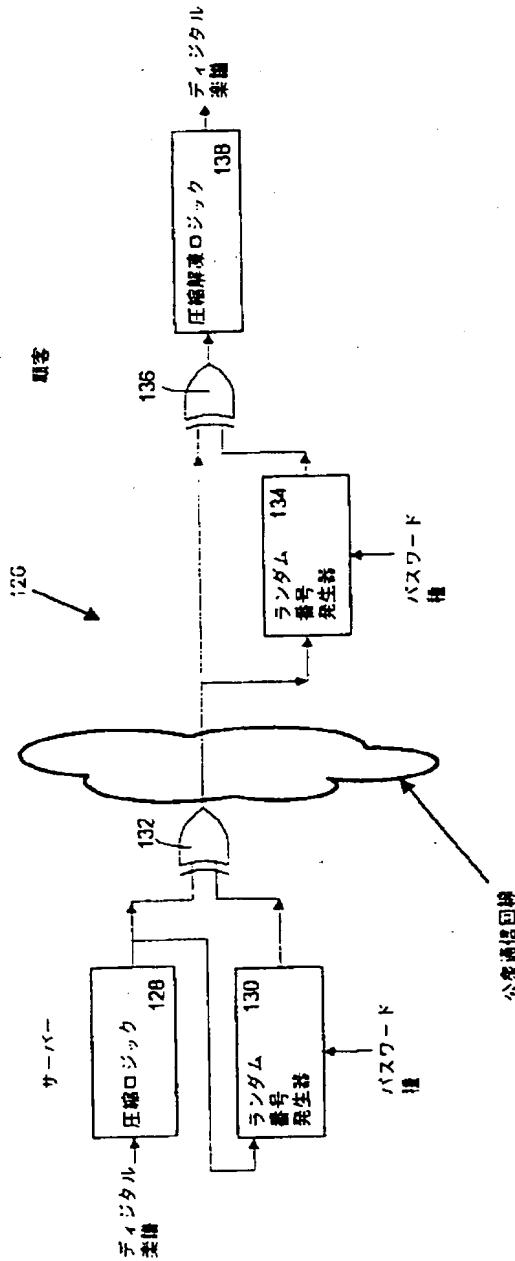
【図6】



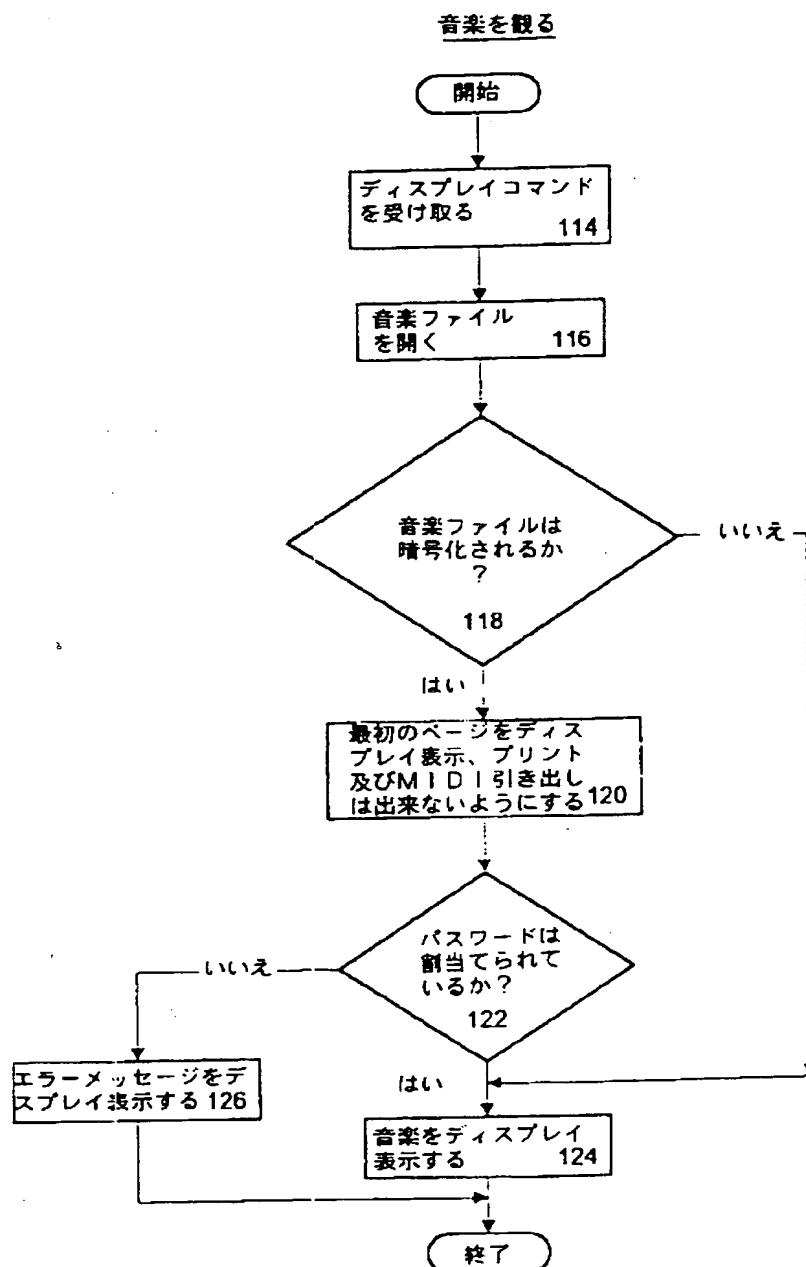
【図9】



【図7】



【図8】



フロントページの続き

(72) 発明者 ブレント アール ミルズ
 アメリカ合衆国 ワシントン州 98115
 シアトル サーティナインス アベニュー
 ノースイースト 7720

【外国語明細書】

ENCRYPTION SYSTEM WITH TRANSACTION CODED DECRYPTION KEY

Field of the Invention

The present invention relates generally to monitoring the distribution of information that is accessible through a public network and, in particular, to a method and system for using key-based encryption to inhibit and track unauthorized distribution by a key holder. The invention has particular application with regard to the commercial distribution of copyrighted works or other proprietary subject matter over a public network.

Background of the Invention

The advent of widely available public computer networks, and particularly public networks capable of supporting multimedia functions such as the Internet, presents a great opportunity for consumers and content providers such as music publishers. Such networks afford content providers increased access to an ever growing market. Consumers benefit from improved access to information and greater convenience. Moreover, in some cases, the digital nature of the information received over a network is preferable to more conventional modes such as printed media. For example, digital sheet music can be printed to replicate its printed media counterpart. Additionally, the digital sheet music can be directly processed by audio and video playback programs, as well as by a variety of digital musical instruments and equipment such as Musical Instrument Digital Interface (MIDI) devices.

Despite this potential, content providers have been reluctant to embrace this market in many cases. One reason for this reluctance has been a perceived threat that access to proprietary subject matter such as copyrighted music over a public network will erode ownership interests in and revenues from such subject matter. The

concern is that unscrupulous persons will wrongfully access such subject matter or that authorized users, having rightfully accessed the subject matter, will thereafter distribute the subject matter in contravention of the content providers' rights. Although such possibilities exist in connection with other modes of distribution, public network distribution is thought by some to present peculiar dangers due to the ease with which widespread distribution can be accomplished, e.g., via bulletin boards and the like.

Indeed, conventional computer security systems developed to control access to restricted access data are not well-suited to address these concerns of content providers. For example, access password systems are somewhat effective in limiting access to designated information, but do not afford protection once the information is transmitted from the server system to a public network. Encryption systems have been devised to prevent use of information that is wrongfully intercepted as a result of transmission over a network. In this regard, in key-based encryption systems, authorized clients are provided with a decryption key. The protected information is then transmitted in encrypted form to prevent use by any intercepting party. The authorized client receives the encrypted information and uses the decryption key to decrypt the information. Unfortunately, such encryption systems generally do not provide adequate safeguards to discourage the authorized clients from subsequently redistributing the protected information.

Summary of the Invention

The present invention is directed to a method and system for controlling access to protected information from a server, as well as discouraging and tracking subsequent redistribution of such information after it has been transmitted from the server. The invention facilitates commercial distribution of proprietary subject matter through public or open networks by providing improved protection of proprietary rights and increasing the likelihood that infringing activity will be corrected.

Moreover, the invention provides increased marketing flexibility by allowing for limited, multiple-use authorization and pre-purchase sampling of copyrighted works or other confidential subject matter. The invention also provides a novel, encryption on-demand capability which, it is believed, has not been feasible in connection with physical storage media such as CD-ROM and magnetic storage media.

According to one aspect of the present invention, a method and corresponding system is provided for monitoring distribution of information accessible over a public network on a client-specific basis. The method includes the steps of: establishing a database of information at a server; encrypting at least a portion of the information using a key-based encryption system; in connection with a request by a client, assigning a client-specific key to the client; and transmitting the key to the client. The client-specific key includes some indicia that can be used to identify the client, thereby allowing for monitoring of information use on a client-specific basis.

The database can include various types of information, for example, digital sheet music, literary or artistic works, software programs, or other subject matter transmittable in digital form. Any identifying information can be coded into the key for client identification. Examples include: personal or financial data provided by the client; address information for the clients' computer or web site; account numbers or serial numbers; other information for identifying the computer used by the client; and abbreviated or encoded versions of any of the above. Conveniently, such information can be stored in a separate client database and indexed to the key. Preferably, the decryption system requires entry of the key each time the protected information is used (i.e., the system does not store the information in decrypted form) and appends the client identifying information to any redistributed digital or hard copies of the information. In this manner, the client is discouraged from redistributing the protected information because the key is required to use the information in its original digital form, and distribution of the key or an identified hard copy may involve disclosure of sensitive information or otherwise create a traceable record of the

client's infringing activity.

According to another aspect of the present invention, a method and corresponding system is provided for enabling transaction-specific access authorization with respect to protected information. The method involves the use of a key-based encryption system, such as generally discussed above, where decryption keys are assigned on a transaction-by-transaction basis. That is, decryption keys are assigned on demand in connection with a transaction involving communication of the protected information from the server to a client. For example, the transaction may involve the purchase of a copy of sheet music, a digital musical score or other protected information, or it may involve paying a license fee to use such information a designated number of times, for a designated duration, or during a designated license term. The key can include information sufficient to identify the subject information and/or the client. The invention thereby allows for transaction-specific authorization and increased marketing/distribution possibilities.

According to a further aspect of the present invention, partially encrypted information is transmitted prior to providing a decryption key so as to allow for sampling of the information before a transaction is consummated. In particular, the associated method involves establishing a database of information at a network server, encrypting a portion of the information and receiving an access request. Upon receiving an access request, a selected portion of the information is transmitted in partially encrypted form and, thereafter, a decryption key is transmitted to the client. By way of example, the partially encrypted information can be sheet music where only the first page of a score is unencrypted for viewing. The client can thereby browse through a selection of scores prior to making a purchasing decision, authorizing payment and, in response, receiving a decryption key.

According to a still further aspect of the present invention, a method and corresponding system is provided for enabling post-transmission monitoring of information use by a client. The method includes the steps of: receiving encrypted

information and storing the information in memory in its encrypted form; receiving a decryption key and storing the key in memory separate from the encrypted information, for example, in a cache; identifying a request by a client to access the information; in response to the request, retrieving the encrypted information and key from memory and, thereafter, decrypting the information; and outputting the information for use by the client. The method can be implemented, for example, by playback/display software running on a client computer. The software can be programmed for limiting access to the protected information according to transaction parameters, *e.g.*, limiting access to the scope of a license purchased by the client. The access request can be an "open file," "display," or "print" message or the like.

In a preferred implementation, the protected information is never saved in its decrypted form but, rather, is only decrypted on a just-in-time basis when the corresponding file(s) is opened for use. Accordingly, redistribution of the information in its decrypted form is discouraged or practically prevented. Moreover, in order to permit third-party use of the information, redistribution of the information in its encrypted form will also require distribution of the decryption key, which may be an unattractive option for the client.

The present invention thus allows for monitoring access to protected information on a server and subsequent use or redistribution by a client. Additionally, the invention allows for tracking of any unauthorized redistribution and thus facilitates enforcement of server rights. The invention also provides for increased marketing/distribution options and novel on-demand decryption key coding. By virtue of these and other advantages, the invention promotes distribution of proprietary subject matter over public networks to the mutual benefit of consumers and content providers.

Brief Description of the Drawings

For a more complete understanding of the present invention and further

advantages thereof, reference is now made to the following detailed description, taken in conjunction with the drawings, in which:

Fig. 1 is a schematic diagram of a computer system in accordance with the present invention;

Fig. 2 is a chart providing a functional overview of the distribution monitoring system of the present invention;

Fig. 3 is a diagram of the Music Viewer download function of the system of Fig. 2;

Fig. 4 is a diagram of the music download function of the system of Fig. 2;

Fig. 5 is a diagram of the on-line music purchase function of the system of Fig. 2;

Fig. 6 is a flow chart of the music printing function of the system of Fig. 2;

Fig. 7 is a flow chart of the music viewing function of the system of Fig. 2;

Fig. 8 is a schematic diagram of the encryption/decryption components of the system of Fig. 2; and

Fig. 9 is a flow chart of the encryption/decryption function of the system of Fig. 2.

Detailed Description of the Invention

The distribution monitoring system of the present invention is useful in a variety of applications where it is desired to monitor the distribution of proprietary subject matter over a public network. In the following description, the invention is set forth in the context of monitoring distribution of digital musical scores over a network. It will be appreciated that this particular application is set forth for the purpose of illustrating the invention, and various aspects of the invention have broader application as defined by the claims below.

Fig. 1 illustrates an encryption-secured computer system 10 according to the present invention. The computer system 10 includes a server 12 that can

communicate with clients 14-20 across a public network 21 such as the Internet. In the case of the Internet, the server 12 can be accessed via the Netscape 2.01 or Microsoft Internet Explorer 3.0, or higher browsers. The server 12 generally includes a processor 22 and a library or database of digital musical scores stored in a memory 24 as files 26-32. As discussed in detail below, the server 12 is operative for receiving access requests from clients 14-20, assigning decryption keys or passwords and transmitting an accessing program and selected scores to the clients 14-20 over network 21. A number of other functions relating to receiving payment, indexing and storing encoded decryption passwords and the like are also performed by server 12.

For present purposes, the clients 14-20 may be considered as being functionally equivalent. Details of only one of the clients 14 are shown in Fig. 1. Generally, the client 14 includes a central processing unit (CPU) 34, an internal cache 36 and/or external cache 38, memory 40 and input/output (I/O) hardware 42, all interconnected via data bus 44. The CPU, which may include any suitable microprocessor, is operative for downloading and running the accessing program, accessing memory 40 and caches 36 and 38, and communicating with I/O hardware 42. In the illustrated embodiment, the CPU 34 also includes a built-in, internal cache for storing the decryption key used to decrypt downloaded musical scores. Generally, cache 36 is an area of extremely fast Random Access Memory (RAM) for storing frequently used or time critical data so as to allow for faster operation. The cache 36 can be accessed more rapidly than memory 40. Alternatively, the decrypting key can be stored in an external cache 38, which may comprise a RAM chip located on the computer motherboard. Memory 40, which is separate from caches 36 and 38, may include computer memory as well as the storage of floppy disks, CD-ROM drives and hard drives. The I/O hardware 42 can include a number of types of devices including a mouse, keyboard or other user input device; a viewing monitor; a printer; or a MIDI device.

Fig. 2 provides a functional overview of a music distribution monitoring system 46 used in connection with the computer system 10 of Fig. 1. As shown in Fig. 2, the monitoring system 46 can be broken down into a number of functions that are executed by logic on the server and/or a client. The functions of the illustrated system 10 include: downloading (48) a music accessing program, in this case designated the "Music Viewer," for use by a client in accessing music files stored on the server; downloading (50) a selected musical score from the server; purchasing (52) music on-line (and thereby obtaining an access license and encoded decryption key); printing (54) and/or viewing (56) the music and music encryption/decryption. It will be appreciated that the music may also be reproduced from digital information using a MIDI device or the like. Each of these functions is discussed in turn below.

Fig. 3 illustrates the Music Viewer download function of one implementation of the present invention. After communication between the server and client has been established through the network, the client initiates the download function by requesting (58) the server to download the program. This request can be entered by following appropriate prompts from the server site. The server receives (60) the download request and sends (62) the Viewer software package to the client. Upon receiving (64) the software package, the client runs the setup code to install the Music Viewer software. In order to access musical scores stored in the server library in the illustrated system, the client is assigned a unique Viewer identification code. Accordingly, the client is prompted to request (66) a Viewer ID as part of the download procedure. In response to the ID request, the server generates (68) a Viewer ID and logs the ID in a Viewer database. The server then sends (70) the newly generated Viewer ID to the client and logs the transmission time and date, the Internet Protocol (IP) address (or similar information for other networks) of the client, and the client's machine name or type (as entered by the client user or determined from a transmission header or the like). The client then receives (72) the assigned Viewer ID and a successful installation is thus completed.

The system of the illustrated embodiment allows the client user to browse through the music library and view a selected portion, e.g., the first page, of musical scores prior to consummating a transaction by purchasing a music copy or paying a license fee. Fig. 4 illustrates the associated pre-purchase music download function. The function is initiated when the client selects a score to sample and requests (74) the music from the server. In this regard, the score may be selected from a list of titles by scrolling through the library and clicking on a selected title, by using a search function to call a title, or by any other appropriate means. The Viewer ID is also sent to the server at this time. Upon receiving the request, the server finds (76) the requested musical score, compresses and encrypts (or partially encrypts) the score as will be described below, and stores the encrypted score in the download area. In addition, the server assigns and logs a decryption key that is unique to the client and also logs an identification code for the score, the download IP, and the Viewer ID for the transmission. For example, the key can be a password composed of two 32 bit numbers where one of the numbers is an index to identify the client in a client database and the other number is random, or encoded with additional information as desired. By indexing the key or password to the client database in this manner, the password can be used to identify the client, look up license or account information and otherwise monitor distribution on a client-specific and transaction-specific basis.

The server then sends (78) the client the Uniform Resource Locator (URL) address of the newly encrypted music. Upon receiving (80) the URL, the client can request (82) a download of the file or files containing the encrypted music. The server then finds (84) the encrypted music in the download area, queues up the music, and downloads (86) the music to the client. The client receives (88) the encrypted music and stores the music in memory, e.g., computer memory, hard drive storage, etc. At this point in the illustrated implementation, i.e., prior to purchase, only the first page of the score is not encrypted. Accordingly, the client user can play and view (90) the first page of the music to verify that the downloaded score is the score

desired by the user and to otherwise evaluate purchasing options.

After thus browsing through the music library and sampling one or more scores, the client user may decide to make an on-line music purchase, e.g., to purchase a copy of the music in sheet music form, or to pay a license fee to print copies, view the music in its entirety, play back the music on the client's I/O hardware, or otherwise use the music. Such a license may be for single use, multiple use, unlimited use during a license term, etc. Fig. 5 illustrates the on-line purchase function. The function is initiated by the client by sending (92) payment information (for example, a credit card account number and expiration date, or the number of a previously established, pre-paid or unpre-paid account with the server institution), the score ID, the download IP, Viewer ID and/or any other information to the server. Some or all of this information may have already been transmitted to the server in connection with browsing the music library and would not necessarily have to be re-transmitted. The exchange of personal and financial information can be encrypted using standard public key encryption as provided, for example, in the Secure Sockets layer of the browser.

Upon receiving (94) this information, the server downloads the score and Viewer ID, and contacts the client user's financial institution or a credit card approval service, looks up balance information, or otherwise obtains authorization for the transaction. Based on the results of this authorization inquiry, the server sends back (96) to the client either a bad payment message (e.g., "payment declined"), or the server sends a decryption password and logs the password and other transaction information in its database. By operation of the Music Viewer software, the client then receives (98) the password and stores the password in a password database separate from the downloaded music. It will thus be difficult for a client user to improperly redistribute music because the user will generally not be aware that a decryption password has been stored in its system, nor will the user know how to access the password. In operation, the Music Viewer software monitors client

messages until it receives (100) an "open file" message indicating that the user desires to print, playback or otherwise use the music. At this time, the Music Viewer locates (102) the password, which may be stored in a client cache for speed of operation. The Music Viewer can also retrieve license information relevant to the client's access request and, in appropriate cases, increment the client use count under the license as discussed below. If the client has remaining uses under a license, the Music Viewer decrypts the score in memory. It will be noted that the music is never saved in decrypted form, but is only decrypted just-in-time for a requested use, thereby discouraging improper redistribution.

Fig. 6 illustrates a music printing function according to the invention. As previously noted, after downloading music and a password, the Music Viewer monitors client messages to identify access requests. When a print command is received (104), the Music Viewer consults its client database to determine (106) whether there are any remaining printouts allowed under the license previously purchased by the client user. In this regard, the client user may have paid a single use or multi-use license fee. If the license has been exhausted, the client is notified (108) accordingly, and information may be provided concerning options for paying a further license fee. Otherwise, the Music Viewer encodes (110) various information regarding the transaction in the user database, e.g., Viewer ID, score ID, download ID, date, time and number of licensed printouts used. This information can be encoded, for example, in a base 72 number string in an appropriate format, and then printed (112) on the copy (e.g., next to the copyright notice). Similarly, this same identification information can be written into a comment statement of a MIDI file to tag MIDI extractions. This information allows for proper incrementing of a multi-use license and also allows for subsequent tracking of any improper redistribution of the printed copy. In this regard, if a printed copy of the score or MIDI file is found, the associated transaction and client can be readily decoded.

Instead of, or in addition to printing the music, the on-line user may desire to

view the music on a monitor. For example, the music may be viewed in conjunction with playing back the music for enhanced enjoyment, or the music may be displayed to facilitate selection of playback options involving tempo, instrumentation and the like. Fig. 7 illustrates the associated music viewing function. Upon receiving (114) a display command, the Music Viewer opens (116) the requested music file and determines (118) whether the file is encrypted. If the music is not encrypted, e.g., because it has been decrypted in a previous step or is public domain music, the music can be directly displayed (124). However, in the case where the music is encrypted with the exception of the first page for sampling, the Music Viewer proceeds to display (120) the first page and disable printing or MIDI extraction. If the client user then attempts to display the remainder of the music, the Music Viewer first determines (122) whether a valid and unexpired password has been assigned to the user. If so, the music is decrypted and displayed (124). Otherwise, an error message is displayed (126).

Figs. 8 and 9 illustrate one implementation of the encryption/decryption function of the music distribution monitoring system. It will be appreciated that any suitable technique, including using a public key encryption/decryption algorithm, can be employed as the base level encryption/decryption technology in accordance with the present invention. In addition, the base level encryption/decryption technology can be implemented in hardware and/or software logic. The following description illustrates one exemplary implementation. Referring first to Fig. 8, the encryption/decryption components are schematically shown. On the server side, the encryption/decryption subsystem 126 includes compression logic 128, random number generator 130 and exclusive OR (XOR) gate 132. The compression logic, which can be a conventional data compression software program or a data compression hardware package, receives the raw digital musical score and compresses the score for transmission. It will be appreciated that this compression, in addition to improving transmission speed, enhances subsequent encryption as the

compressed and encrypted data will be especially difficult for an intercepting party to decipher. The random number generator 130 can include one or more conventional random number generating programs. In this regard, two such programs can be employed to handle the two 32 bit words of the decryption password. The random number generator 130 implements an algorithm for generating a determined series of values starting from an initial seed. In the illustrated embodiment, the assigned password is provided to the generator 130 as a seed. The generator 130 also receives an input from the compressed data stream line that triggers the generator 130 such that the generator 130 outputs a bit stream equal in length to and coordinated with the compressed data stream. The generator output and compressed data stream are used as the two inputs into the XOR gate 132 which performs its characteristic disjunctive comparator function. The output from XOR gate 132 is transmitted over the network to the client.

On the client side, the subsystem 126 includes a client-side random number generator 134 and client-side XOR gate 136, each identical to its server-side counterpart. The subsystem 126 further includes decompression logic 138 that is the logical complement of compression logic 128. The random number generator 134 uses the password as a seed, and generates a bit stream of length determined by an input from the encrypted data stream. It will thus be appreciated that the output bit stream from generator 134 will be identical to that of generator 132, this output, and the encrypted data stream, serve as the two inputs into XOR gate 136. The successive operation of the XOR gates 132 and 136 yield an output from XOR gate 136 that is identical to the output from compression logic 128, i.e., a compressed digital music score. This compressed score is decompressed by decompression logic 138 to yield the digital score in uncompressed, decrypted form. It should be noted that the musical score is decrypted as part of the music output process, not prior to saving the score. Additionally, the encryption/decryption process can be successively performed on page-sized chunks in the case of printing, or on appropriately-sized

portions of an audio output (e.g., two seconds of the score), in order to allow for display/play-back on an as-ready basis.

The encryption/decryption process is summarized in the flow chart of Fig. 9. The process is initiated, on the server side, by receiving (140), or calling from memory, a digital representation of the musical score. The digital representation is then, in sequence, compressed (142), encrypted (144) and transmitted (146) across the network to the client. On the client side, the signal is first decrypted (148) to obtain a compressed digital representation, and then decompressed (150) to obtain the digital score. The score can then be output (152) as desired by the client user.

The following prophetic example illustrates the overall operation of the music distribution monitoring system of the present invention. A client accesses the music distribution server at its World Wide Web site using, for example, the Microsoft Internet Explorer 3.0 browser. From the server home page, the user first selects the option for downloading the Music Viewer program. After selecting this option, the user follows the prompts or instructions to install the software and, in the process, enters various requested identification data. The user may then return to the home page and select the music library option to browse the available selections. The user can then scroll through the available selections to identify a score of interest, for example, "Mozart's Sonata Number 1." In order to verify that this is the piece that the user has in mind, the user may download the score for sampling. The Music Viewer software stores the partially encrypted digital score and will allow the first page of the score (which is transmitted in unencrypted form) to be displayed on the client monitor and played back.

After one or more scores are thus sampled, the user may decide that he desires to print, view or otherwise use a digital score and that he therefore desires to purchase a copy of or pay a license fee for the score. The user can then select a purchase function and a menu of purchase options will be provided, e.g., single print license, multi-print license, unlimited viewing license for a given license term, etc.

The user selects the desired option, responds to a series of prompts concerning identification information and payment information, e.g., by entering a credit card number and personal information. If payment is approved, the user will be assigned a decryption password that is indexed to the client's identifying information in a client database held by the server. By way of example, the client may pay a license fee for ten printouts. In the same or subsequent sessions, the client can request a printout under the license. The system will keep track of the number of printouts used and allow printing only so long as the license is unexhausted. Whenever the user prints out a copy of the score, an encoded string of characters is printed next to the copyright notice.

An unscrupulous user may attempt to redistribute the music with disregard for the server/copyright holder's rights. Having the downloaded music file on his system, the user may attempt to redistribute the music electronically. However, having thus attempted to wrongfully redistribute the music, the user will discover that the redistributed information cannot be used because it is encrypted. Such a user may attempt to break the encryption code and may even ultimately surmise that a key has been stored in the client's memory somewhere separate from the music file. In the unlikely event that the user should succeed in redistributing the music together with the password in useable form, the infringing user will have unwittingly left a record of his infringing activity in the form of the personal information that can be derived from the client/transaction encoded password. Similarly, redistribution of printed copies or MIDI files will provide a record due to the coded character string included with the copyright notice or in comment statements. In any event, the coded information facilitates enforcement and thus discourages infringement.

While various embodiments and applications of the present invention have been described in detail, it is apparent that further modifications and adaptations of the invention will occur to those skilled in the art. However, it is to be expressly understood that such modifications and adaptations are within the spirit and scope of

the present invention.

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)
THIS PAGE BLANK (USPTO)
copy

CLAIMS

1. A method for use in monitoring distribution of information accessible through a public network said information included in a database at a server of said public network, comprising the steps of:

encrypting at least a first portion of said information using a key-based encryption system, said key-based encryption system requiring entry of a key to decrypt said encrypted information;

in connection with a request by a network client, assigning a first client-specific key to said client for decrypting said encrypted information, said first client-specific key including at least a first identifier useful for identifying said client; and

transmitting said first client-specific key to said client, wherein said key can be used to monitor distribution of said information on a client-specific basis.

2. A method as set forth in claim 1 wherein said information comprises a digital musical score and said step of encrypting at least a portion of said information comprises retaining a second portion of said digital musical score in an unencrypted form so as to allow for sampling of said digital musical score prior to decryption.

3. A method as set forth in claim 1 wherein said step of assigning said first client-specific key comprises acquiring identification information regarding said client and encoding said identifier with respect to said acquired identification information.

4. A method as set forth in claim 3 wherein said identifier comprises a password that is indexed to a client database including said identification information.

5. A method as set forth in claim 3 wherein said identifier includes information for identifying client equipment.

6. A method as set forth in claim 3 wherein said identifier includes information for identifying a client user.

7. A method as set forth in claim 1, further comprising the step of transmitting said encrypted information to said client prior to said step of transmitting said first client-specific key.

8. A method as set forth in claim 1, further comprising the step of transmitting accessing software to a client, said accessing software being operative for allowing said client to access said information in said database.

9. A method as set forth in claim 8, further comprising the step of employing said accessing software to print a copy of said information.

10. A method as set forth in claim 8 wherein said information comprises a digital representation of a musical score, and said method further comprises the step of employing said accessing software to play back said musical score.

11. A method as set forth in claim 8, further comprising the step of displaying said information.

12. A method as set forth in claim 1 wherein said step of assigning said first client-specific key is conducted in response to receiving said request by said client.

13. A method as set forth in claim 1, further comprising the steps of storing said information in a first area of memory and storing said first key in a second area of memory separate from said first area, wherein said information and said first key can be separately accessed.

14. A method as set forth in claim 1, further comprising the steps of storing said information in a client memory in encrypted form, receiving a request to output said information, and decrypting said encrypted information in response to said output request.

15. A method as set forth in claim 1, further comprising the steps of receiving an access request from a second network client requesting access to said information and assigning a second client-specific key, different from said first client-specific key, to said second client for decrypting said encrypted information.

16. A method as set forth in claim 1, further comprising the step of using said first client-specific key to track subsequent redistribution of said information.

17. A method as set forth in claim 1, further comprising the steps of outputting an output copy of said information and embedding identification information in said output copy, wherein said identification information facilitates tracking of redistribution of said information.

18. A computer system for use in monitoring distribution of protected information accessible through a public network, comprising:

a first area of memory for storing a database including said protected information;

a controller operative for receiving an access request from a network client requesting access to said protected information, obtaining identification information useful for identifying a source, and assigning a decryption key using said identification information; and

encryption logic for encrypting said protected information based on said decryption key wherein said decryption key is useful for decrypting said encrypted protected information.

19. A computer system as set forth in claim 18, further comprising a second area of memory for storing said identification information, wherein said identification information is indexed to said decryption key.

20. A system as set forth in claim 18 or 19 wherein said controller is further operative for receiving payment information from a client, wherein said decryption key is assigned in response to receiving said payment information.

21. A system as set forth in claim 18, 19, or 20 wherein said protected information comprises a digital musical score and said encryption logic is operative for partially encrypting said score.

22. A system as set forth in claim 18, 19, 20, or 21 wherein the source is said network client.

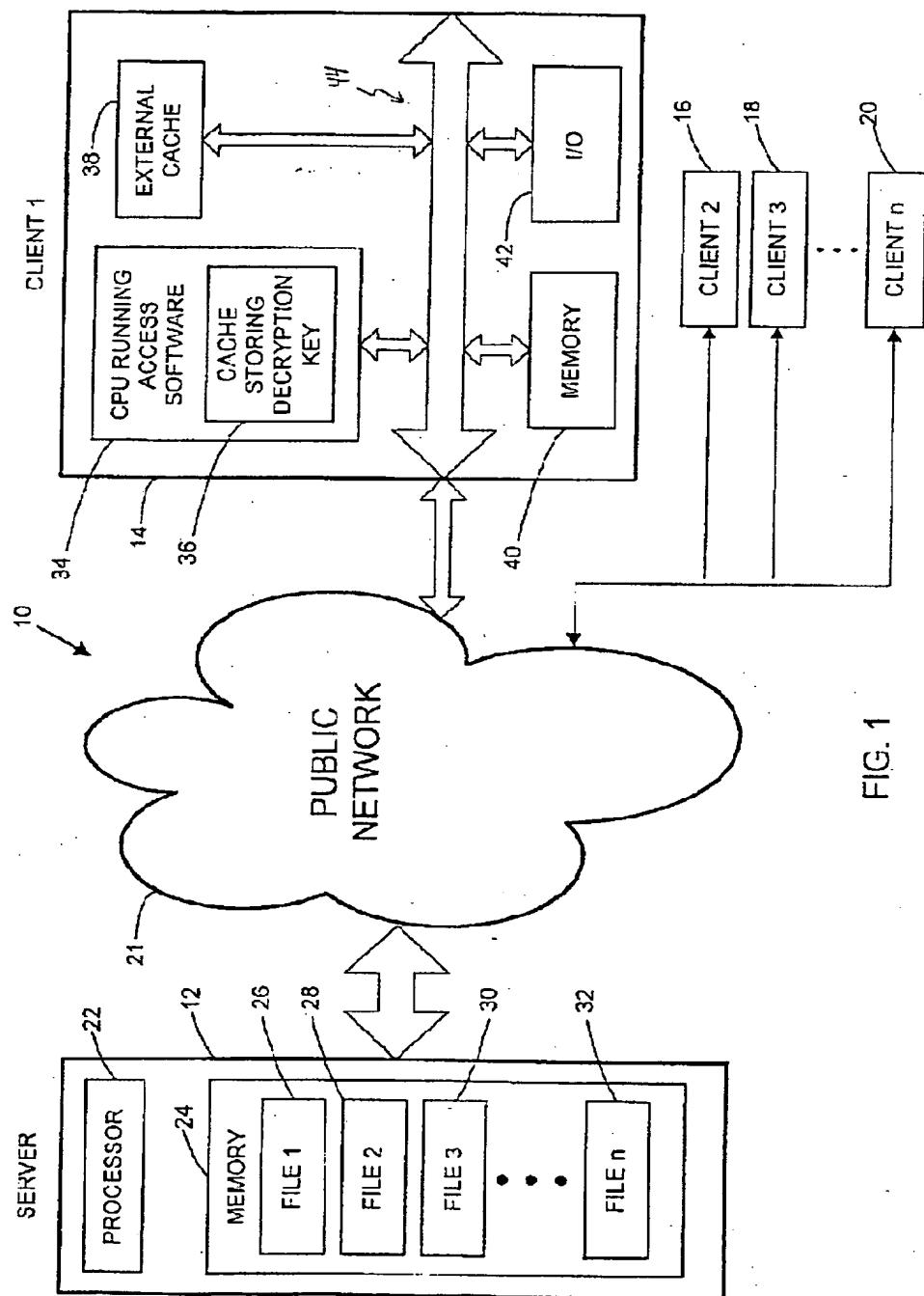


FIG. 1

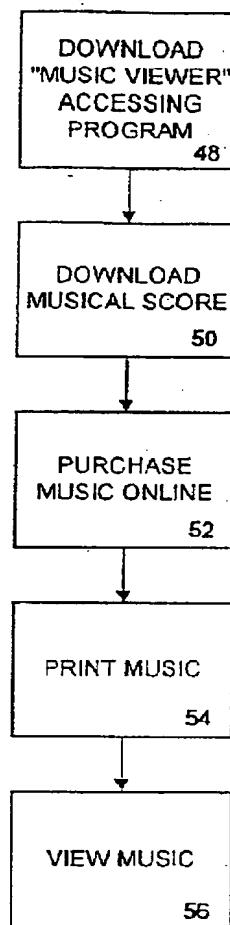
2
SYSTEM OVERVIEW

FIG. 2

3

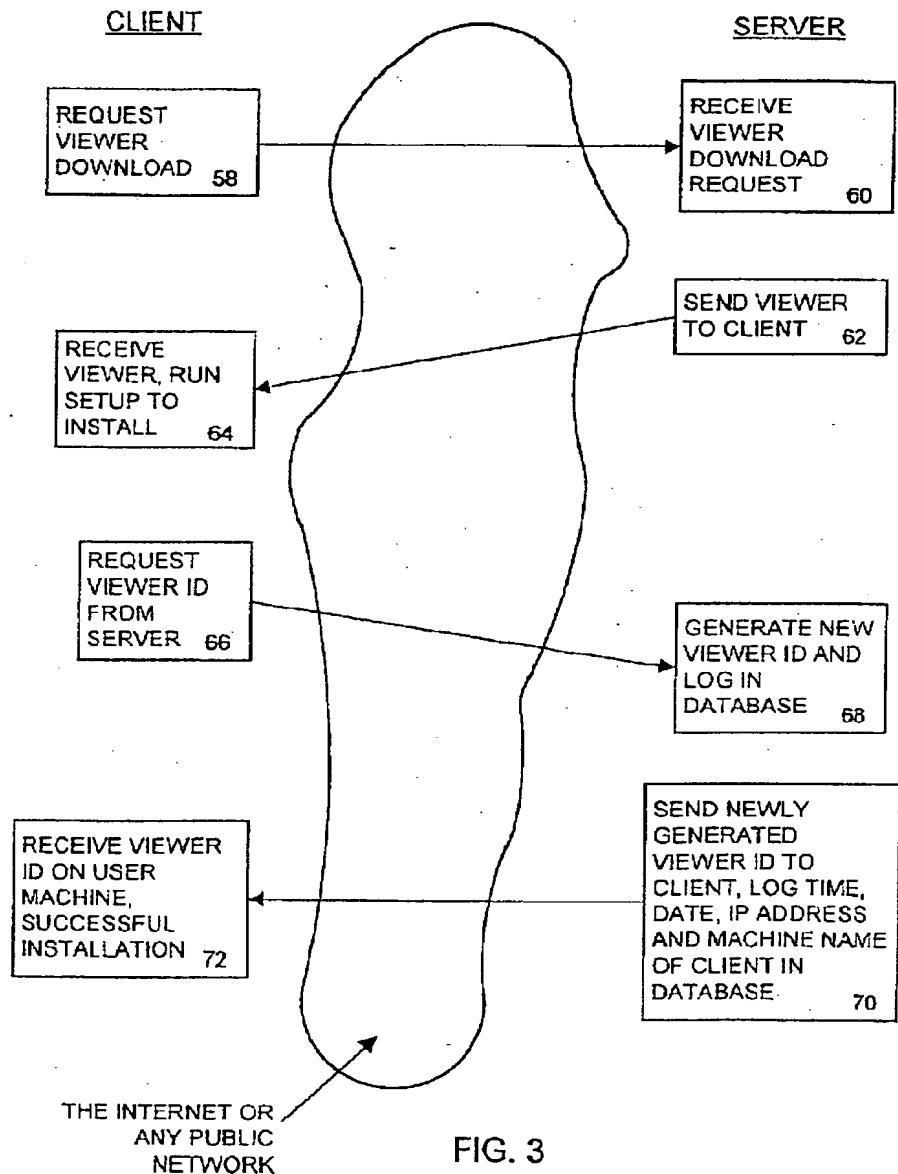
MUSIC VIEWER DOWNLOAD

FIG. 3

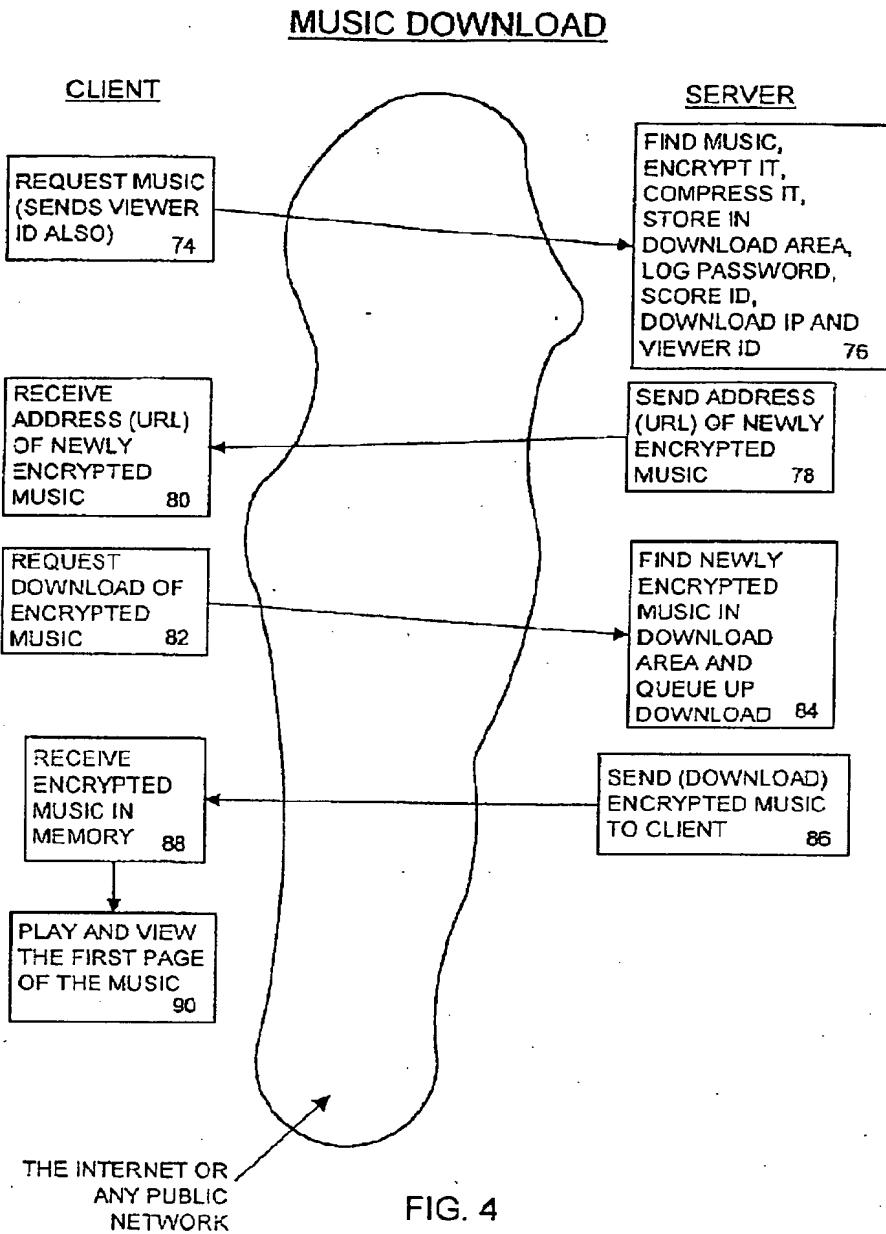
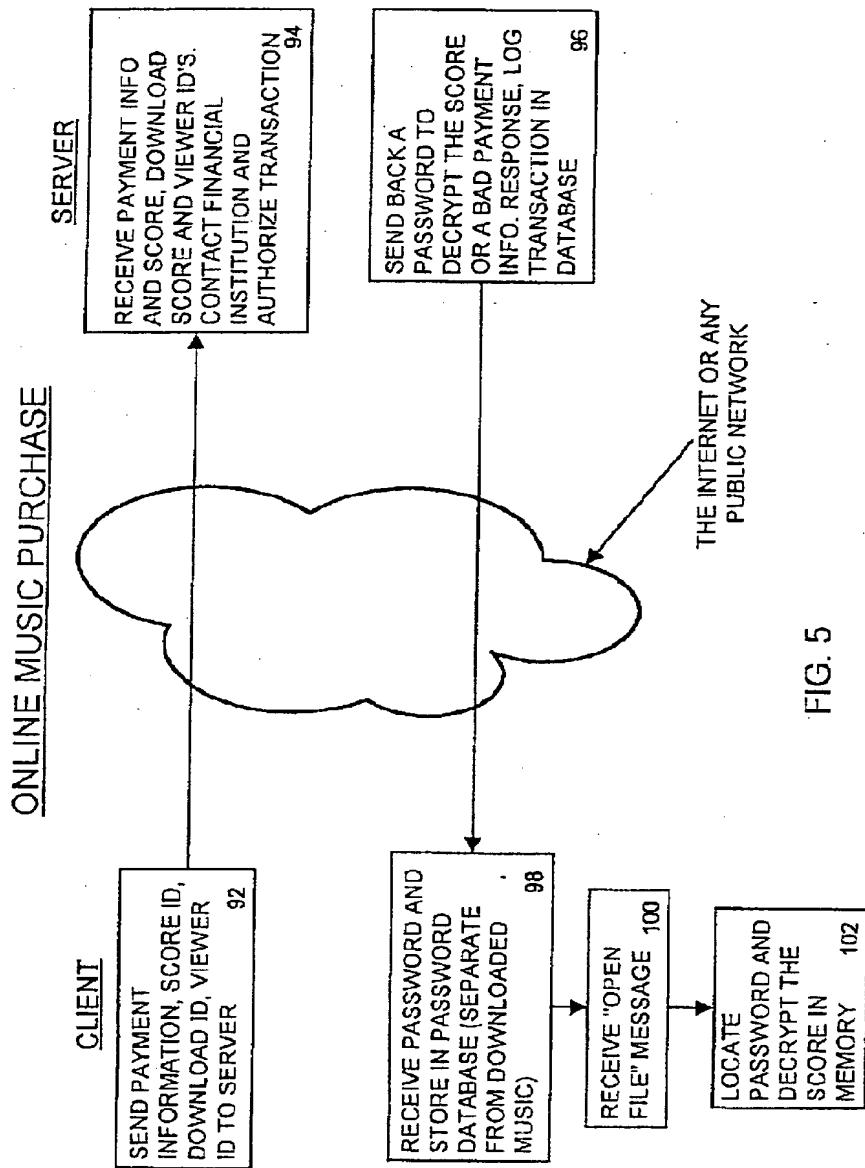


FIG. 4



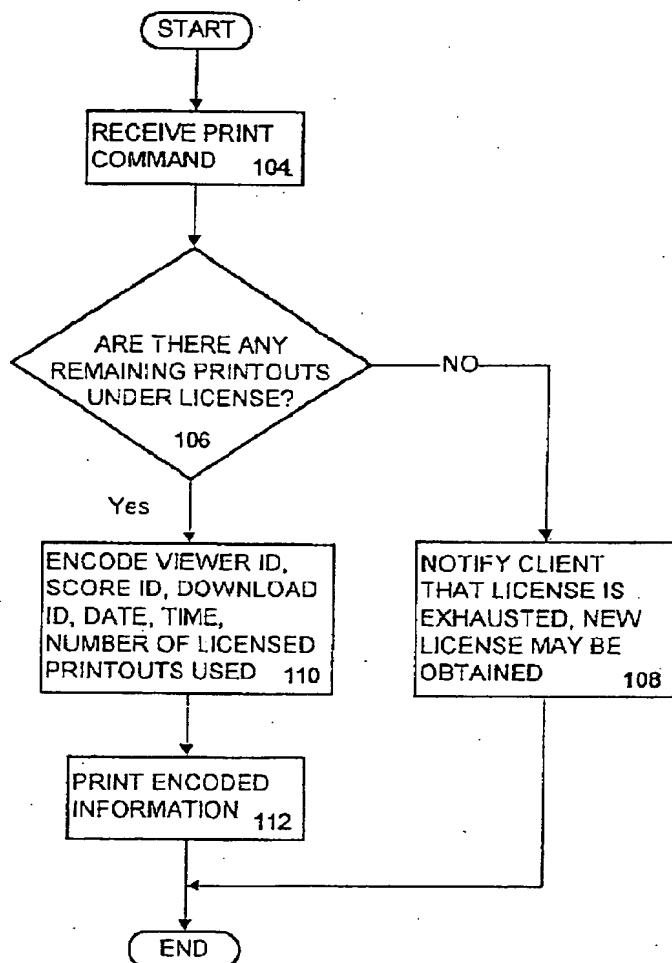
PRINTING MUSIC

FIG. 6

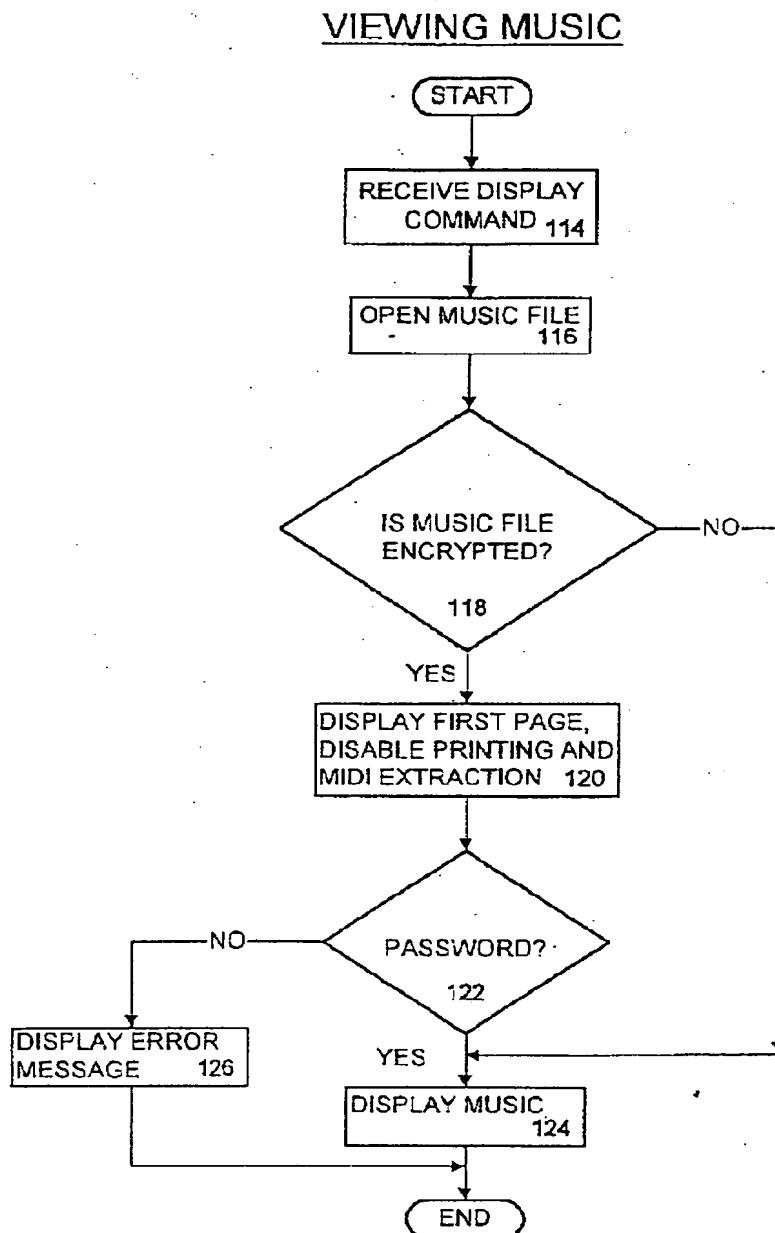


FIG. 7

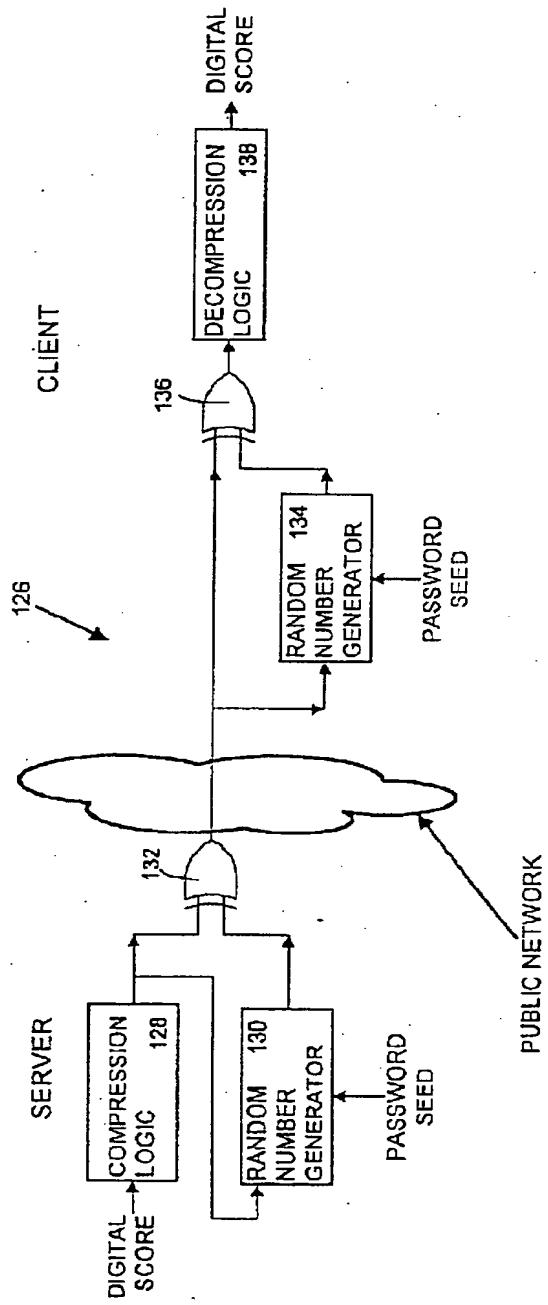


FIG. 8

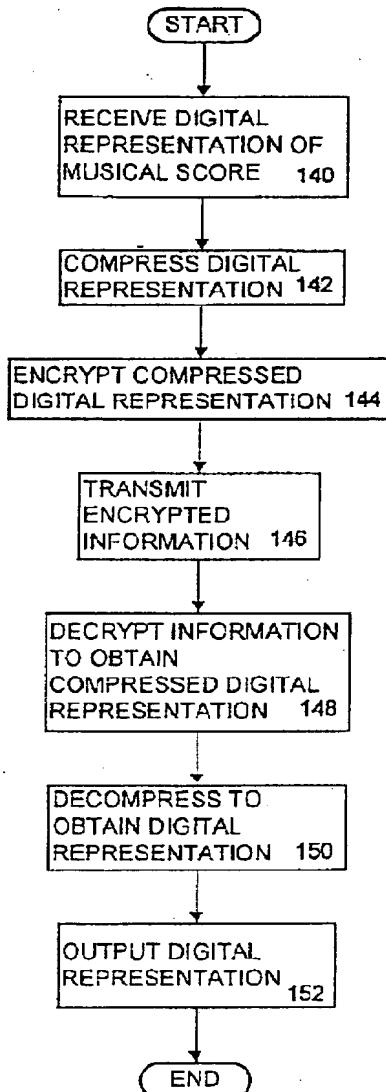
ENCRYPTION/DECRYPTION

FIG. 9

Abstract of the Disclosure

ENCRYPTION SYSTEM WITH TRANSACTION CODED DECRYPTION KEY

The encryption secured computer system (10) includes a server (12) that communicates with clients (14-20) across a public network (21) using a novel transaction coded decryption key technology that discourages wrongful redistribution of protected information such as digital musical scores, and allows for tracking of infringing activity. In one implementation, the server (12) distributes access software and partially encrypted musical scores to clients upon request. A client can sample the partially encrypted scores prior to consummating a transaction. When a score is selected, the client enters payment information and is assigned a password that is specific to the client and transaction. The password functions as a decryption key to enable use of the musical score by the client employing the access software. Any subsequent wrongful redistribution of the musical score together with the decryption password can be traced due to client identifying information encoded into the password.

THIS PAGE BLANK (USPTO)